The New Netwar:

Policy Exchange

Countering Extremism Online

Dr Martyn Frampton
with Dr Ali Fisher and Dr Nico Prucha

Foreword by General David H. Petraeus (US Army, Ret.)

The New Netwar:

Countering Extremism Online

Dr Martyn Frampton
With Dr Ali Fisher and Dr Nico Prucha

Foreword by General David H. Petraeus (US Army, Ret.)

Policy Exchange

About the Authors

Dr Martyn Frampton is a Reader in Modern History at Queen Mary University of London. He is the author of three books on 'the Troubles' in Northern Ireland and more recently has completed a major book on the history of the relationship between the Muslim Brotherhood and the West, which is due to be published by Harvard University Press in late 2017. He has also written on the contemporary challenges of counter-terrorism, most significantly with the Policy Exchange publications, 'Choosing our Friends Wisely: Criteria for engagement with Muslim groups' (2009) and 'Unsettled Belonging: A survey of Britain's Muslim communities' (2016).

Dr Ali Fisher is Explorer of Extreme Realms at *Human Cognition.* He specializes in delivering insight into complex information ecosystems through innovative approaches, network analysis, and big data. In the past 10 years Ali has worked with a range of organisations seeking to track and counter the behavior of extremists online and illegal uses of the internet. Ali built BlackLight which has delivered data on core ISIS communication networks. He has written numerous articles on Public Diplomacy and Strategic Communication and a book *Collaborative Public Diplomacy*, which examines collaborative strategies for dealing with complex problems.

Dr Nico Prucha is Chief Content Curator at *Human Cognition*. He is a fluent Arabic speaking specialist in Jihadist theology and strategy. His work has covered the use of the internet by Jihadist groups from the mid-2000s to the present and documented shifts in strategy from Forum to Twitter to Telegram. Main aspects of his research cover the relationship of textual and audio-visual content of jihadist activity online, specifically focusing on the extremist definition of applying theology. Another major focus is the understanding and analysis of the social media strategies used by groups such as the Islamic State in theory and practice. His blog is available at www.onlinejihad.net.

Acknowledgements

The authors wish to thank Martin Boon of ICM Unlimited who gave invaluable advice and assistance with the framing of the public polling. Lord Carlile of Berriew likewise provided many valuable insights that helped to clarify our thinking. We also wish to thank Hannah Stuart, Gabriel Elefteriu, Julia Mizen, Amy Gray, Martin Kendrick and Dean Godson of Policy Exchange for their help in bringing the project to fruition. Nico Prucha would like to thank Madhat and Majid, Abu Zaynab and Haydar; and pay tribute to the many Arab voices that are unheard and shouting in the dark.

Published by
Policy Exchange, 8 - 10 Great George Street, Westminster, London SW1P 3AE
www.policyexchange.org.uk

ISBN: 978-1-910812-34-1

Contents

Executive Summary

Policy Exchange's new report provides a comprehensive analysis of the struggle against online jihadist extremism – what we call "the new Netwar". This issue is vital to UK national security and there is a danger that the blood and treasure we are investing in defeating ISIS in Iraq and Syria will produce little more than a pyrrhic victory unless we act to defeat the virtual threat. At present, we are certainly not winning the war online. The spate of terrorist attacks the UK suffered in the first half of 2017 confirmed that online extremism is a real and present danger. In each case, online radicalisation played some part in driving the perpetrators to violence. As a society, we are struggling to grasp the extent of the challenge and also appropriate ways of responding. It is clear that the status quo is not working. It is time for a new approach. Policy Exchange has worked with a team of experts to provide fresh insight into the debate around online extremism. The report that follows is divided into three sections:

Part One: 'Swarmcast' – the Use of the Internet by the Jihadist Movement:

In this first part, Dr. Ali Fisher and Dr. Nico Prucha examine the nature of the online challenge posed by the Sunni extremist (jihadist) movement. The key findings of the section include:

The Role of Theology

- Contemporary ISIS-inspired content draws on a cohesive and long-established theological narrative, which attempts to position jihadists as the only "true" Muslims.
- ISIS proclaims its objective as the "caliphate upon the prophetic methodology", justifying all of their actions by reference to selectively chosen religious scripture, tradition and scholarly interpretation.
- The content released by ISIS is overwhelmingly in Arabic, yet this content is rarely addressed and remains under researched.
- Non-Arab recruits to ISIS have been used to explain what life is like in an "Islamic State" and glorify different aspects of the jihad – social and civic dimensions, as much as the violent cutting edge.

Content Production

- The decline of ISIS in the online space has been significantly overstated – the movement has maintained a consistent virtual output and presence throughout the last three years.
- Conservatively, the movement produces around 100 pieces of new content in an average week (and often much more than that). This adds to an ever-growing archive of material built up over three decades.
- Videos are a critical part of ISIS' online output, enabling the group to overcome language barriers and propagate key messages. To-date ISIS has produced around 2,000 'official' videos. This number rises to 6,000 when the wider jihadist movement is included.
- In many cases, content production is decentralised – driven by ISIS' autonomous 'provinces'. This feature has been missed, or under-appreciated by other analyses of the movement.
- Analysis of this process shows that ISIS content production has been largely consistent over the long-term. It has survived the death of key figures, the loss of territory and ongoing fighting.

Dissemination

- Jihadist content is disseminated online by means of a 'Swarmcast' – an interconnected network that constantly reconfigures itself, much like a swarm of bees or flock of birds in mid-flight. That Swarmcast is defined by its speed, agility and resilience. It has allowed ISIS and their sympathisers to outmanoeuvre all efforts to-date to reduce significantly their online presence.
- Core jihadist content is transmitted to the vanguard by the use of Telegram, which plays host to a rich array of textual and audio-visual extremist content.
- The jihadists engage in outreach and missionary work, by means of mainstream social media platforms – which are used to disseminate the core content to a wide audience. While Telegram exists as a 'safe haven' for jihadists, they have not abandoned other platforms such as Twitter, Facebook and YouTube.
- Twitter accounts for 40% of the identifiable traffic to jihadist content online. Extremist content is also regularly accessed via Facebook, Google and Telegram.
- Tens of thousands of users access jihadist content from all over the globe. For the content analysed in this study, the UK is the fifth most frequent location from which the content was accessed (after Turkey, the US, Saudi Arabia and Iraq) – and the most frequent location in Europe.
- The media and some academics are, by their actions, inadvertently making ISIS material more 'findable' and durable. Making ISIS content more 'findable' undermines the efforts of those who are attempting to restrict access to extremist material.

- 'Whack-a-mole' approaches on the part of the security services have been unable to disrupt the strategic dissemination of content, which remains consistent.

Part Two: What is to be done? Options for Future Policy

The second part of the report builds on the recognition that existing counter-measures are not succeeding and that jihadist content continues to be disseminated online at a consistent rate. It considers different options for disrupting the strategic objectives of the jihadist movement and looks towards a comprehensive approach that will tackle the 'supply chain' of extremism at both ends. The report acknowledges that there is a need for balance and proportionality – to avoid the undue 'securitisation' of western societies. Yet equally, a core theme is the need for society – as a whole – to take responsibility for tackling this problem. Key proposals include:

- A new ethical code of conduct for researchers, by which they pledge not to re-post original jihadist content in unadulterated form – and especially not in real-time.
- Measures for drying up the supply of extremist content online – principally by pushing the technology companies to do more. There has recently been a groundswell of criticism for perceived failings of the mainstream social media corporations when it comes to tackling extremist material. Whilst there have been signs of limited change from the companies, concrete action of a kind that would genuinely transform the situation remains elusive.
- To this end, we suggest how the government might pursue an approach based on 'responsive regulation', which pushes the tech companies to accept their responsibilities and take decisive action. As a start-point, those companies should be treated as de facto publishers and distributors of online content.
- Building on this, we outline a graduated, six-step plan of measures by which the government could put pressure on the leading tech companies to improve their performance:
    - Ask the companies to revise and implement more stringent codes of conduct/terms of service that explicitly reject extremism
    - Require the companies to work with and fund the efforts of an expanded Counter Terrorism Internet Referral Unit (CTIRU)
    - Empower the forthcoming Commission for Countering Extremism to oversee content removal online
    - Establish a new independent regulator of social media content, within the purview of Ofcom
    - Put in place a system of financial penalties, administered by the independent regulator, to force company compliance

- Consider ways in which the existing legislation against the distribution of extremist material can be used to prosecute repeat offenders from the tech companies

- At the other end of the supply chain, we recommend that the government find new ways to reduce 'demand' – by targeting those who wish to consume extremist material. At present, the legal framework for dealing with this issue is fragmented. There is also no prohibition on the consumption or possession per se of extremist content.
- We recommend that the government consider creating a new legal framework for dealing with this problem. One option would be to develop civil remedies – perhaps by extending mechanisms such as the Terrorism Prevention and Investigation Measures (TPIMs), or revisiting proposals for 'Extremism Disruption Orders'
- Alternatively, the government could consider new legislation that would criminalise the 'aggravated possession and/or persistent consumption of material that promotes hatred and violence in the service of a political ideology'.
- Such powers would need to be framed carefully to avoid any undue infringement of civil liberties, but the scale of the challenge requires innovative thinking and a bold new approach.

Part Three: Assessing Public Attitudes

The need for change was underscored in the final part of our report, which presents the findings from a major new survey of public attitudes towards the challenge of online extremism. The purpose of this exercise was not to prove, in a crude way, that x, or y policy was popular – but rather to illuminate public thinking on this still-new and ever-evolving issue. We aimed to understand:

a) The extent to which the public *is* worried about extremist content disseminated via the internet;
b) The degree to which there is an appetite for a new approach to this problem;
c) The way in which public views about online extremism correspond to underlying attitudes about the internet, and questions about the need for security and liberty.

Key findings from the polling include:

- 65% of respondents believe that the major internet companies are not doing enough to combat online radicalisation; only 14% thought they were doing enough on this issue.
- 74% of people feel that the big internet companies should be more proactive in locating and deleting extremist content.
- 72% of respondents said it was the internet companies' responsibility to control or remove extremist content.

- There is strong public support for a range of measures to tackle extremist content online.
- 75% would support the creation of an independent regulator akin to Ofcom, to monitor online content.
- 74% of respondents would support new legislation to criminalise the persistent consumption of extremist content online; 73% would support legislation to criminalise the possession and viewing of extremist content. In each case, at least 66% of respondents supported the idea that this could include the handing down of prison sentences.
- 66% of people believe that the internet should be a regulated space in which extremist material is controlled; only 25% feel that it should be "completely free" without any limits on free speech.

In presenting these and other findings, the authors hope that this report can help initiate a major new - and necessary - policy debate about online extremism. As a society, we must seek a new consensus on:

- the balance between liberty and security
- the role of the State in relation to the internet
- the moral and social norms that are appropriate to the digital age

This report is offered as a critical contribution to this most pressing challenge: the effort to win the 'new Netwar' and overcome the challenge from online extremism.

Foreword

General David H. Petraeus (US Army, Ret.)

The fight against ISIS, Al Qaeda, and the other elements of the global jihadist movement has become the defining struggle of the early 21st Century. That struggle has increasingly been contested not just on the ground, but in a new domain of warfare, cyberspace.

In the sixteen years since the 9/11 attacks on the American homeland, we have engaged Islamist extremists on numerous foreign battlefields – most notably in Afghanistan, Iraq, and Syria. We have also seen attacks on the home fronts of many NATO allies and partner countries around the world. A number of appalling incidents in recent years have underscored the magnitude of the dangers at home – with three jihadist-inspired terrorist attacks in the UK alone claiming the lives of 35 people so far this year. The attempted bombing of an underground train in London last Friday – using a device that can be built from instructions available online – merely underscored once again the ever-present nature of this threat.

Of course, the UK does not stand alone in the face of this challenge. In the United States, we have seen devastating attacks in Orlando, San Bernardino and Boston. Allies such as Belgium, France, Germany and most recently, Spain, have also been targeted, as have friends and partners beyond the shores of Europe and North America. The intent and the capacity of our enemies to do us harm has been made very clear.

Today, US and British armed forces, working closely with NATO allies and coalition partners from around the world, are helping to drive ISIS out of its last major redoubts in Iraq and Syria. Whether the ongoing campaigns takes weeks or months to complete, few now doubt that the ISIS 'caliphate' will be eliminated and the bulk of ISIS' forces in those countries defeated. Sadly, however, it is clear that the struggle will not end there, but will have to be prosecuted in other locations as well – and that our efforts will have to be sustained, as this is likely a generational endeavor. The events of the last decade-and-a-half attest to the durability and adaptability of the jihadist movement.

I have seen how the defeat of jihadist forces in one theatre does not equate to victory in the overall struggle – or, sadly, even to enduring success in that theatre. When I was privileged to command the Multi-National Force-Iraq during the 'Surge' of 2007 and 2008, coalition and Iraqi forces largely destroyed al-Qaeda in Iraq (ISIS' forerunner) and

the associated Sunni insurgent groups, killing or capturing key leaders, promoting reconciliation with many of the rank and file members, and driving the groups out of their key strongholds in the Sunni areas of Iraq. By the time US combat forces withdrew from Iraq in late 2011, ISIS was incapable of carrying out significant operations without rejuvenation and reconstitution. Unfortunately, although the achievements of the Surge were sustained for over three years, enduring success proved elusive. Highly sectarian actions by the Iraqi government at the end of 2011 and in 2012 alienated and inflamed Sunni communities in Iraq. Reinvigorated by the Sunni opposition and fuelled by exploitation of the Syrian civil war, al-Qaeda re-emerged as ISIS and carried out combined arms combat operations to conquer a broad swathe of territory in northeastern Syria and northwestern Iraq. Meanwhile, an al-Qaeda affiliate was also established in northwestern Syria, capitalizing on the fertile fields for extremism created by the civil war.

The al-Qaeda-ISIS jihadist movement has survived and spread around the world by dint of its adaptability, malleability, and capability to exploit local dynamics. It has operated at various times and in various places as a quasi-State, an insurgency, a terrorist movement, and an ideological project – in some cases operating as all three simultaneously. As in the child's game of whack-a-mole, when pushed down in one place, extremist elements often pop up in another. Jihadists have shown particular facility in exploiting ungoverned or even inadequately governed spaces in the Islamic world. And now, as this new Policy Exchange report shows, they are also exploiting the vast, largely ungoverned spaces in cyberspace, demonstrating increasing technical expertise, sophistication in media production, and agility in the face of various efforts to limit its access.

The threat posed by jihadist extremism online has, in fact, metastasized in recent years. During that time, it has evolved into a scourge that blights the internet and allows jihadists to reach into our societies and to tear at the very fabric of them. The magnitude of the problem has grown dramatically; as I stated at an event in Sydney earlier this year, the 'virtual Caliphate' is a problem that western governments – and social media platforms and internet service providers – must address much more than has been the case to date. This domain of the fight against jihadists may well be the longest campaign of what has been termed 'the long war', and it is vital that the concepts to guide it – and the tactics and techniques to prosecute it – are developed further.

It is clear that that our counter-extremism efforts and other initiatives to combat extremism on line have, until now, been inadequate. In fact, I do not think we have yet developed all the 'big ideas' needed to come to grips with the problem, much less the policies and methods to combat it. Given that, this valuable new study from Policy Exchange is very timely and very useful.

The authors of this report agree that we are not winning the 'new Netwar'. They contend that we have been drawn into fighting on our enemy's terrain and have consistently been responding to their

initiatives and innovations, rather than forcing the enemy to respond to our initiatives and actions – never a good situation in which to be. Efforts to counter online extremism have, in fact, generally failed to advance beyond tactical, ad hoc, and reactive responses. Recent initiatives announced by some media platforms and service providers are of course welcome. Nonetheless, as the authors explain, we need to see delivery on promises. More generally, we need to develop a more coherent, more comprehensive approach than at present, one in which the different sectors of government, business, and society work together, debate and develop overall approaches, and do their part in the ongoing campaign against extremism.

Social media platforms, internet service providers, and other tech companies clearly have central roles to play in the effort to counter extremist groups in cyberspace. Without wishing to understate the difficulties they face, I think it is fair to ask whether their efforts to-date have been commensurate with the scale of the challenge. As this report documents, there is something of a crisis of public confidence on this issue. Two-thirds of the British people, for example, believe the leading tech companies are not doing enough to combat online radicalisation, and three-quarters of them want those companies to do more to locate and remove extremist content. The public expect – and deserve – more from the most powerful and wealthy internet corporations.

Major social media and internet firms exert considerable influence over the way we live our lives. It does appear, however, that there needs to be greater clarity than at present about the obligations that accompany such power. Governments can also play a critical role here, of course, by thinking creatively about how the new media should be regulated and what national and perhaps supranational policies should be established.

It is evident too that when it comes to discussions about online extremism, we need to ask ourselves difficult questions and contemplate uncomfortable answers. Do police and security services have the powers that they need to combat the threat? What more can we do to 'raise the bar' in terms of de-incentivizing the possession and consumption of extremist content? At a broader level, do we have the balance right, between freedom of speech and privacy rights on the one hand, and security on the other? And how far should democratic governments interpose themselves into the online space?

These are not all questions that can be solved purely in a UK or US context. They clearly resonate on both sides of the Atlantic and also across the English Channel and around the world – and a true solution to the problem of online extremism will require joined-up, international collaboration. There is, however, no doubting the urgency of this matter. The status quo clearly is unacceptable.

Policy Exchange's report is, I believe, a vital contribution to this debate. It serves as a catalyst and departure point for much needed discussion amongst policy makers, security practitioners, social media and internet providers, and the general public in the US as well as in Britain. Indeed, policy makers around the world dealing with this key dimension of the contemporary struggle against extremists will find

considerable value in this study. My hope, needless to say, is that this report – and others like it – will spur all of them to do much more than is being done at present to address the ever-changing scourge of online extremism.

General David H. Petraeus (US Army, Ret.) is a Partner in the global investment firm KKR and Chairman of the KKR Global Institute, a Judge Widney Professor at the University of Southern California, a member of the board of Optiv (a global cyber security services firm), a Senior Fellow at Harvard University's Belfer Center, and an investor in over a dozen technology startups. Before joining KKR, he was Director of the Central Intelligence Agency, a position he assumed after concluding a distinguished 37-year military career with six successive commands as a general officer, including command of the International Security Assistance Force in Afghanistan, US Central Command, and the Multi-National Force–Iraq during the Surge.

Introduction

In recent years, there has been a growing recognition of the challenge posed by online 'radicalisation'. This issue has risen to the top of the public policy agenda and the Prime Minister, Theresa May, has made clear that she sees it as a priority. As the bureaucratic structures of the "Islamic State" (ISIS) are driven out of its last remaining urban or metropolitan strongholds in Iraq and Syria, it is increasingly clear that the battle against Sunni extremism – jihadist extremism – must be won in the intellectual, and especially virtual terrain, as much as in the physical world.

Despite the recent focus on the putative decline of ISIS, the UK experienced three successful jihadist attacks in the first half of 2017, and there have been numerous foiled plots over the last several years. Beyond our borders, ISIS and members of the wider jihadist movement have claimed responsibility for attacks in France, Belgium, Indonesia, Bangladesh, Nigeria, Libya, Iran, Yemen, Afghanistan, the Philippines and Egypt. Few would anticipate the disappearance of violent jihadist extremism in the near-to-mid-term.

This is an issue of fundamental importance to UK national security. In addition to the immediate physical threat, the jihadist movement has a proven capacity for using online space to reach into western communities. A key target audience has been the most vulnerable sections of society. This phenomenon has of course been dramatised by instances of 'homegrown' radicalisation, which preceded actual attacks – or by the departure of British citizens to join ISIS. Perhaps the most infamous example of the latter was the case of the east London 'jihadi brides'.[1] In addition, there have been reports of extremist online recruiters targeting converts and subjecting them to a process of 'grooming', in an effort to persuade them to travel to Syria or carry out attacks here in the UK.[2]

In each of these cases, the internet played a critical role in the recruitment and mobilisation of individuals to the jihadist cause. Statistics show that this is a real and growing problem. Altogether, in over a third of terrorist convictions between 1998 and 2015, the internet played a major role as a site of radicalisation. Over two-thirds (69%) of Islamist-related terrorism offences in the UK have been committed by individuals who were known to have in some way consumed extremist and/or 'instructional' terrorist material. This includes: being found in possession of extremist and/or instructional material on arrest; having viewed such material (typically with other cell members); or having produced and disseminated such material. The proportion of offences where the offender consumed extremist

1 Vikram Dodd, 'Four London schoolgirls who left UK for Syria married men approved by Isis', *Guardian*, 19 January 2016, https://www.theguardian.com/world/2016/jan/19/four-london-schoolgirls-who-left-uk-for-syria-married-men-approved-by-isis.

2 Ben Farmer, 'Former glamour model "groomed online as jihadi bride"', *Daily Telegraph*, 4 September 2016, http://www.telegraph.co.uk/news/2016/09/04/former-glamour-model-groomed-online-as-jihadi-bride/;
Lizzie Dearden, 'Isis "jihadi brides" trying to radicalise girls and encourage UK terror attacks online as they remain trapped in Syria', *Independent*, 13 August 2016, http://www.independent.co.uk/news/world/middle-east/isis-jihadi-brides-women-british-syria-kadiza-sultana-radicalise-terror-trapped-abuse-married-air-a7187946.html.

and/or instructional material rose to 76%, for the period 2011–2015, as compared to 63% between 1998 and 2010.[3]

Leading jihadist publications are now a feature of almost every major security service investigation. Where once it was *Inspire* that Western commentators identified as animating the would-be terrorist's mind, today the breadth of production also includes well-known magazines such as *Dabiq* and *Rumiyah*, as well as news updates from Amaq, al-Bayan, and ISIS announcements in their familiar blue and red colour scheme. However, these outlets are only the tip of a very large iceberg. There is a vast and authoritative archive of content at the core of the jihadist movement produced by media foundations like al-Wafa' and al-Himma, the various ISIS wilayat (provinces) and associated media outlets. This vast archive of highly complex content cannot be wished away – any more than we can wish away the physical manifestations and actions which this content seeks to justify and inspire. Increasingly, it seems self-evident that what happens online does not stay online.

A recognition of the importance of online content has led the UK and its allies to target the physical manifestations of 'virtual' extremism. In late 2015, drone strikes actively targeted, and killed ISIS members known to be prominent as online radicalisers and recruiters. The deaths of Reyaad Khan and Junaid Hussain drew new attention to the danger posed by people who could provide ideological inspiration and practical assistance to would-be terrorists via the online space.[4] Nevertheless, such military-based responses are – by their very nature – extremely rare and in themselves, do not address the fundamental problem: the ready availability online of easily found and clearly effective extremist content. This issue is one that can only be addressed by a reduction *online*, in the availability and findability of that content – as a necessary corollary of the military fight.

It is hard to overstate the importance of this task. If we neglect the online networks that jihadists use to disseminate their coherent theological framework, it is likely that ISIS will endure even after their formal governing and bureaucratic structures are removed. General Joseph Votel, head of U.S. Central Command, which oversees military operations in the Middle East, told the *Los Angeles Times* that ISIS' loss of territory did not mean it was on the verge of absolute collapse. Instead, he predicted that the group would continue to coordinate and inspire attacks from its online 'virtual caliphate'. 'The military defeat of ISIS', he argued, was 'essential but not sufficient'. Votel went on to state that, 'as we continue to degrade ISIS' physical capability they will shift more of their attention to the virtual realm and we will need to do whatever we can to stay ahead of them.'[5] Faced with retrenchment in the real world, the jihadists will surely rely on arguably their most potent weapon: the projection of influence by their media operations and the coherent narratives these purvey.[6]

In many ways, the challenge is not a new one. The jihadist movement has been active online since at least the 1990s. Yet for too long, much discussion remained trapped in rather sterile debates about whether the internet mattered as a form of interaction and recruitment

3 Hannah Stuart, 'Islamist Terrorism: Key Findings and Analysis', Henry Jackson Society, March 2017, p. 10, http://henryjacksonsociety.org/wp-content/uploads/2017/03/Islamist-Terrorism-key-findings-and-analysis.pdf.

4 On these airstrikes, see Intelligence and Security Committee of Parliament, UK Lethal Drone Strikes in Syria, HC 1152 (26 April 2017).

5 W.J. Hennigan, 'The U.S. military is targeting Islamic State's virtual caliphate by hunting & killing its online operatives one-by-one', Los Angeles Times, 5 May 2017, http://www.latimes.com/world/middleeast/la-fg-isis-online-20170502-story.html.

6 For ISIS, the phase of conquest and consolidation of territory starting in 2013 has produced 'a generation of firm believers God granted the benefit to be raised in the [restored] abode of Islam (dar al-Islam). A generation brought up without distortion of their religious creed and their natural composition as believers'. ISIS sees this as a firewall against physical defeat and loss of territory. See, Abu Anas al-Jaza'iri, al-'adhb al-namir fi l-tahrid 'ala l-hijra wa-l hathth 'ala l-nafir, al-Wafa', June 29, 2017.

within the jihadist movement. The plain fact is that, over the last two decades, the movement has developed techniques to expose individuals they have never met to their theology, strategy, and tactics by the publication of a range of materials distributed in both digital and hard copy versions.

More recently, it is clear that the security agencies have recognised the threat from online extremism and have taken various steps to try and 'improve their game'. In 2007, for instance, Europol created a 'Check the Web' project to 'share information on Islamist terrorist activities'. The Clean IT project backed by the European Commission in 2010 further attempted to reduce the impact of terrorist use of the internet.[7] In the UK, the Association of Chief Police Officers launched the 'Counter Terrorism Internet Referral Unit' (CTIRU), to identify and flag extremist and terrorist-supporting content to the platform providers hosting it – an effort joined by a EUROPOL unit with a similar remit.[8] In 2016, the European Commission unveiled a "Code of Conduct on Countering Illegal Hate Speech Online" as part of the EU Internet Forum.[9]

Nonetheless, there is a strong sense that these counter-measures: a) barely scratch the surface of online radicalisation; and b) are always one step, or more, behind those whom they are trying to check. Officials speak wearily of the effort to get 'upstream' of the threat – but there is scant evidence that they feel confident of succeeding.

A report co-authored by the Centre of Religion and Geopolitics and Digitalis has suggested that Britain and its allies are losing the war against online extremism.[10] Others have argued that ISIS is winning the conflict on social media at a 'strategic level'.[11] The truth of these assessments raises a troubling prospect: at a time when we have invested significant blood and treasure in the fight to defeat ISIS in Iraq and Syria, will the physical disaggregation of the group in the Middle East prove little more than a pyrrhic victory?

The difficulties of combatting the extremist threat online are, in part, a function of the scale of the challenge. The vast quantity of extremist material 'out there' has forced the authorities to limit their focus to the most egregious content. In addition to this, it is evident that the security services have run into serious difficulties, when trying to encourage social media and online communications companies to adopt a more rigorous approach towards extremism. The companies have deferred to arguments about 'free speech' – and, in an effort to deflect responsibility, have overstated their own inability to effect radical change.

Yet equally, it is time to recognise that current interpretations of online jihadist activity have failed to grasp the strategy, structure, ability, and theology of this movement – to understand properly the way it operates online and the implications of this offline. In the words of Rüdiger Lohlker: 'Without deconstructing the theology of violence inherent in jihadi communications and practice, these religious ideas will continue to inspire others to act, long after any given organized force, such as the Islamic State, may be destroyed on the ground'.[12]

7 The Clean IT project, http://www.cleanitproject.eu/.
8 House of Commons, Home Affairs Select Committee, Radicalisation: the counter-narrative and identifying the tipping point: Eighth report of session, 2016-2017 (25 August 2016) § 24.

9 European Commission code of conduct on countering illegal hate speech online,http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

10 Frank Gardner, 'UK losing online extremism battle, research suggests', BBC News, 31 March 2017, http://www.bbc.co.uk/news/uk-39448987.

11 Audrey Alexander, 'How to Fight ISIS Online', Foreign Affairs, 7 April 2017.

12 Rudiger Lohlker, 'Why Theology Matters – The Case of ISIS', Strategic Review, July–September 2016, http://sr-indonesia.com/in-the-journal/view/europe-s-misunderstanding-of-islam-and-isis.

As this report will demonstrate, jihadists are pursuing a form of 'Netwar'. ISIS and other jihadist groups have established their 'electronic *ribat* (front)' through a wide range of digital media and the media mujahidin stand in constant readiness to engage online. As described in part one, they deploy a user-curated 'Swarmcast', which relies on a vast ecosystem of platforms, file sharing services, websites and social media. The effect of this is to make jihadist content production highly resilient.

Much western commentary fails to appreciate the character and significance of this content – particularly in terms of its theological grounding. The reality is that jihadist 'narratives' are highly coherent and consistent, allowing them to link, for instance, their attacks on the shrine of Ayatollah Khomenei in Iran, to parallel operations in Syria and Europe. This coherency is appealing and enables the online 'Swarmcast' to re-organize and adapt to changes in context.

In response to all of this, the UK and its allies have been drawn into a chaotic and largely ineffective game of 'whack-a-mole' against ISIS and other purveyors of jihadist theology and hate speech The Home Affairs Select Committee reported in August 2016 that the CTIRU had secured the removal of more than 120,000 pieces of terrorism-related content.[13] By one early-2017 estimate, Twitter had taken down 360,000 accounts because of terrorism-related concerns since the middle of 2015. Yet as this report demonstrates, the impact of these 'victories' has been negligible.[14] Policy-makers have also recognised that 'counter narratives' are failing to check the extremist output.[15]

Due to the tactical focus on takedowns and "counter-narratives", the U.K. and its Western allies are being drawn into open warfare online, a battlefield chosen by their jihadist adversaries. And it is the jihadists who will thrive in the chaos that results. The ideology of the jihadist movement, offering a coherent worldview while gaining and consolidating territory, has proven time and again to be resilient on all layers on the internet.[16]

Of course, this is not a purely UK-problem. Yet our key allies show little sign of having developed a more strategic approach. Thomas Joscelyn, a senior fellow at the nonpartisan Foundation for Defense of Democracies in Washington, told the *Los Angeles Times* that 'The U.S. government needs a systematic campaign to undermine the messaging, … So far any effort to do that has flat out failed.' In addition, a US Government Accountability Office study released in April 2017 found 'no cohesive strategy with measurable outcomes has been established' by the US Government for counter-propaganda against ISIS.[17]

Rising to the challenge that online jihadists pose is of vital importance to national security, and we cannot afford to exhaust finite resources removing one piece of media content at a time.

13 House of Commons, Home Affairs Select Committee, *Radicalisation: the counter-narrative and identifying the tipping point: Eighth report of session, 2016-2017* (25 August 2016), §25.

14 Audrey Alexander, 'How to Fight ISIS Online', *Foreign Affairs*, 7 April 2017.

15 Mark Mazzetti and Michael R. Gordon, 'ISIS is Winning the Social Media War, U.S. Concludes', *The New York Times*, 13 June 2015, http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=0.

16 Ali Fisher and Nico Prucha, 'ISIS is Winning the Online Jihad Against the West', *The Daily Beast*, 1 October 2014, http://www.thedailybeast.com/articles/2014/10/01/isis-is-winning-the-online-jihad-against-the-west.html.

17 W.J. Hennigan, 'The U.S. military is targeting Islamic State's virtual caliphate by hunting & killing its online operatives one-by-one', *Los Angeles Times*, 5 May 2017, http://www.latimes.com/world/middleeast/la-fg-isis-online-20170502-story.html.

- **Challenging the jihadist movement online requires a paradigm shift to a more strategic approach, which recognises the role of theology and focuses primarily on disrupting the networks that distribute, acquire and consume content *tout court*, rather than the removal of individual images or accounts.**
- **This will require a collective effort based on collaboration between many elements within our society – and ultimately, without international allies. This will not be easy, but we have no choice if the new Netwar is to be won.**

Moreover, it should be recognised that the struggle against online extremism raises broader questions, with which western society has only begun to grapple. The last two decades have seen the transformation of communications technology. Debates about how to harness the enormous benefits that this has brought, whilst dealing with the problems that have emerged, are still in their infancy. As a society, we are still groping towards answers:

- **about the balance between liberty and security;**
- **about the role of the State and the extent to which it should interpose itself into this sphere; and**
- **about the moral and social norms that are appropriate to the digital age.**

It was against this backdrop, that Policy Exchange brought together a team of experts to reflect on the challenges posed by online extremism. The aim was to provide an in-depth assessment of the struggle against online extremism – and also to reflect on policy options for the future. This report therefore combines several elements. In part one, Dr Ali Fisher and Dr. Nico Prucha were commissioned to provide a survey of the online context. They examine the information ecosystem which the jihadist movement has developed, showing how ISIS continues to produce and distribute content, and the historical sources upon which they draw. Their work includes the largest ever study of the way in which ISIS exploits the social media site 'Telegram' using data collected via BlackLight (a data collection service built by Dr Ali Fisher at Human Cognition) over an 18-month period. The authors have collected and analysed what is likely to be the most comprehensive archive of primarily Arabic propaganda material anywhere in the world, featuring: over 6000 videos; over half a million documents collected over the past two decades; and materials from the 1980s, including historical books, which were digitalised by jihadist media pioneers in the early 2000s.

In part two, we build on the preceding analysis to examine current responses to the online threat and the extent to which these responses are failing to address the full-scale of the challenge. Rather than constituting a meaningful strategic response, they represent ad hoc, tactical adjustments, which do not come close to overcoming the

danger. A key contention would be that the defeat of online jihadist extremism will require a comprehensive, all-of-society, strategic approach. With this in mind, we consider different policy options that might allow us to tackle the different components of the existing threat. Again, the focus here is on trying to identify a comprehensive approach, in which each section of society takes responsibility for the part it can play in defeating online extremism. This indeed, is the core theme of our various proposals: the need for a greater sense of social responsibility – across society as a whole – which will allow everyone to pull together for the common good, in overcoming this pernicious and present danger. Cliched as it may sound, the safety of the individual citizen can only be secured by a collective effort.

Part three focuses on the results of a major new survey that we commissioned from ICM Unlimited, examining public attitudes to the virtual space. If the danger from online extremism is to be surmounted, then it is vital that public opinion is kept 'onside' and that we operate at the level of public understanding – whilst simultaneously trying to educate people as to the nature of the threat. Furthermore, as already mentioned, the challenge of dealing with online extremism forces us to confront a much broader set of issues about how society deals with the new virtual space – which occupies an ever greater part of our lives. In this context, it is crucial both to understand how people see the internet and the problems discussed here.

By drawing these issues together into a single report, we hope that this can feed into a new debate about the way to combat online extremism. We do not presume to think that we have all the answers – but in what follows, we offer a diagnosis of the key problems faced. Our hope is that, by asking questions and raising certain issues, this report can contribute to the emergence of a new and effective strategy for countering online extremism.

Part One: 'Swarmcast': the Use of the Internet by the Jihadist Movement

*Dr. Ali Fisher and Dr. Nico Prucha**

At the dawn of mass access to the internet, some, including author Douglas Rushkoff, foresaw that dissident groups would use technological innovation and the networks of our postmodern society in unconventional ways and toward subversive goals.[18] Similarly, John Arquilla and David Ronfeldt predicted the coming revolution in their seminal work *The Advent of Netwar*:

> This revolution is favoring and strengthening network forms of organization, often giving them an advantage over hierarchical forms. The rise of networks means that power is migrating to nonstate actors, because they are able to organize into sprawling multiorganizational networks (especially 'all-channel' networks, in which every node is connected to every other node) more readily than can traditional, hierarchical, state actors. This means that conflicts may increasingly be waged by 'networks', perhaps more than by 'hierarchies.' It also means that whoever masters the network form stands to gain the advantage.

Today, it is jihadist groups such as ISIS who appear to have the upper hand. They operate in a vast information ecosystem and have developed a multiplatform distribution system – projecting a unique set of coherent content to their followers, sympathisers, and target audience. ISIS has adopted an approach similar to that which Rushkoff outlined in his book *Cyberia*.[19] For ISIS, the 'battle for your reality' is one of religious identity.[20]

The threat posed by extremist material online is real and pervasive. It has a home in large clusters of Arabic dominated networks and builds on the literal tradition established by the first Arab foreign fighters in Afghanistan and later al-Qaeda (AQ). Online content is often part of the process, but it works in combination with other influences, including personal relationships and previous experiences. Access to content shared online may come through an individual searching the web for content in isolation, but equally, results from the distribution of content from ISIS core producers to an influential individual elsewhere, who can download it and subsequently use the material to engage others and attract them to the cause.

** Ali Fisher and Nico Prucha would like to dedicate this section of the report to all those who have died as a consequence of terrorism, violence and conflict. Many Westerners associate terrorism in September with the 9/11 attacks on New York and Washington DC. However, for many communities around the globe – from Afghanistan to Nigeria, from The Philippines to Cameroon – September marks their own moments of tragedy, when loved ones were killed through innumerable acts of violence. In contributing to a report published in September we remember all the victims of terrorism and are mindful of those caught in the crossfire between terrorists and those who fight against them.*

18 Douglas Rushkoff, Cyberia: Life in the Trenches of Hyperspace, (New York: Harpercollins Publishers, 1995) (reprint).

19 Ibid.

20 Further discussed in: Nico Prucha, 'IS and the jihadist Information Highway – Projecting Influence and Religious Identity via Telegram', Perspectives on Terrorism, Vol. 10, No. 6 (2016), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/556.

This online content poses a serious threat to UK national security and cannot be properly understood if the magazines published in English are analysed in isolation and not contextualised into the overall jihadist mindset of hundreds of thousands of Arabic writings and over 6,000 videos. Entry-level content, such as *Inspire* and later *Dabiq* and *Rumiyah* are embedded within a much wider, theologically-inspired hinterland.

The Content of Jihadism: The Importance of Theology

The contemporary jihadist movement inhabits a theological universe that developed over the preceding three decades. That theology is based on complex religious principles; is offered mainly in Arabic; and draws on a range of influences, from the 1980s, down to contemporary ideologues. Jihadist writings and videos refer to and cite, not only religious scripture – selected *ayyat* (verses) from the Qur'an and *Sunna* (deeds and sayings ascribed to Prophet Muhammad) – but also historical Sunni Islamic scholars such as Ibn Taymiyya, Muhammad ibn 'Abd al-Wahhab, Ibn al-Qayyim or Ibn Nahhas. All in all, the jihadist 'archive' might be said to comprise over half a million documents in digital format and mainly in Arabic (materials from before the age of mass digitalization were digitalized by the first generation of committed electronic media mujahidin in the 2000s).

Following 9/11, the internet became the preferred platform for AQ to spread its brand of Sunni extremist theology. This theology entered a new evolutionary phase when ISIS declared a 'Caliphate' in 2014.[21] This AQ offshoot then became the central organisation's primary rival, developing a massive foothold on social media sites – first Twitter[22], now Telegram – while AQ lost significant support, both online and offline.[23] AQ has the ideological seniority, projected by senior jihadist scholars (*shuyukh al-jihad*) such as Abu Qatada al-Filistini, or Abu Muhammad al-Maqdisi, who criticised ISIS' declaration of an Islamic state and disagreed with the killing of the captured Jordanian combat pilot Mu'adh al-Kasasiba. ISIS, by contrast, has the practical edge, having managed to translate territorial control and alleged governance into a coherent online output.

ISIS uses AQ's theology in two ways. The first is through 'applied theology', documented by the massive number of videos released throughout the past three years. What AQ only theorised, ISIS implements and records. Secondly, ISIS re-publishes AQ theological writings (including lengthy books, articles, religious guidelines, legally binding documents (fatwas) and military handbooks). Under Abu Bakr al-Baghdadi, ISIS[24] adopted AQ's iconography and doctrine, without being subject to its formal leadership.[25]

21 'Statement regarding the Relationship of the Qa'idat al-Jihad group to ISIS' (in Arabic), Markaz al-Fajr li-l I'lam, https://alfidaa.info/vb/showthread.php?t=92927. Al-Qaeda Central issued this statement distancing themselves from the Islamic State of Iraq and al-Sham with the refusal of ISIS' leader Abu Bakr al-Baghdadi to pledge allegiance (*bay'a*) to AQ-*amir* Ayman al-Zawahiri. As a consequence, the Syrian revolution against al-Assad was further divided with various 'rebel' factions turning on each other – including *Jabhat al-Nusra*, the official branch of AQ turning on ISIS and vice versa. The clash – or *fitna* (tribulation) – between ISIS and JN as well as other factions is the manifestation of two torrents: the claim of seniority posed by AQ and its Syrian franchise *Jabhat al-Nusra* versus the practicality of the "Islamic State" which advanced what AQ pledged to fight for: the establishment of a Caliphate. Joas Wagemakers refers to ISIS as the *Zarqawiyyun*, practical military orientated individuals who seek to implement their principles of faith by brute force versus the *Maqdisiyyun*, adherents of Abu Muhammad al-Maqdisi who criticised the "Islamic State" for its apparent rapid move in declaring a Caliphate. See Joas Wagemakers, *A Quietist Jihadi – The Ideology and Influence of Abu Muhammad al-Maqdisi*, (Cambridge University Press: Cambridge, New York, Melbourne, 2012). Cole Bunzel referred to this rift as "two tendencies predominate among jihadis insofar as the Syrian war is concerned: one favoring the al-Qaeda-affiliated Jabhat al-Nusra (JN) and cooperation with all rebel groups, and another favoring ISIS and its exclusionary political designs as the reborn Islamic state, or proto-caliphate." Cole Bunzel, 'The Islamic State of Disunity: Jihadsim Divided', *Jihadica*, 30 January 2014, http://www.jihadica.com/the-islamic-state-of-disunity-jihadism-divided/. See also Khalil Ezzeldeen and Nico Prucha, 'Relationship between ISIL and local Syrian rebels break down', *IHS Jane's Islamic Affairs Analyst*, Islamic World Web Watch, April 2014.

22 Ali Fisher, 'How Jihadist Networks Maintain a Persistent Presence Online', *Perspectives on Terrorism*, Vol. 9, No. 3 (2015), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/426.

23 Jabhat al-Nusra (JN), the Syrian AQ affiliate was first to use Twitter on a noticeable scale and facilitated the social media platform to disseminate propaganda videos and writings. The JN-IS divide caused JN to lose members, fighters, and media activists to the "Islamic State". See Nico Prucha and Ali Fisher, 'Tweeting for the Caliphate – Twitter as the New Frontier for Jihadist Propaganda', *CTC Sentinel*, June 2013, http://www.ctc.usma.edu/posts/tweeting-for-the-caliphate-twitter-as-the-new-frontier-for-jihadist-propaganda.

24 At the time the "Islamic State" referred to itself as dawlat al-Islamiyya fi l-'Iraq wa-l Sham (ISIS), then shortened its name after the declaration of the Caliphate to IS or dawlat al-khilafa.

25 Cole Bunzel, 'The Islamic State of Disobedience: al-Baghdadi Triumphant', *Jihadica*, 5 October 2013, http://www.jihadica.com/the-islamic-state-of-disobedience-al-baghdadis-defiance/.

Today, the daily content released by ISIS, or that produced in English, together represent just a fraction of the total jihadist output. It is the wider archive of Sunni extremism, which really reveals the strategy of the movement and the justification for its actions.

Little that ISIS says is new. For example, the archive of the jihadist movement contains the rationale for when female suicide bombers are permitted and when they are not, stretching back to fighting with the Soviets in Afghanistan.

Similarly, one prominent video that is part of the extremist ecosystem features Abdullah 'Azzam – one of the most influential advocates of jihad in Afghanistan – delivering a Friday sermon (*khutba*) in Seattle, in the United States, in 1988.[26] In the film, 'Azzam not only tried to recruit his listeners for jihad against the Soviets, but also attacked the US as another major, and logical future enemy of the Muslims. 'Azzam's *khutba* provided a usual mix of citations from the Qur'an and *Sunna,* bound to contemporary tales of the fighting mujahidin, as well as descriptions of how Muslims were suffering in Afghanistan. 'Azzam repeatedly stressed the need to 'establish an Islamic state', stating that this could only be realised by jihad and combat (*qital*). All of these are themes that are effectively redeployed today by ISIS.

The documents and videos produced by jihadists project an image of what they consider to be a real Sunni Muslim – someone following the path of God, who acts in accordance with divine rules and regulations, as did the early Muslims under the leadership of Prophet Muhammad.

Any release by ISIS – as much as by al-Qaeda before it – seeks to inform, educate and convince the consumer that the jihadis are the only "true" Muslims.

Jihadists try to portray themselves as God's spokespeople. Every piece of their often-times highly professional and sometimes sophisticated propaganda is part of a greater puzzle, which is itself underpinned and scripted by theology. The videos aim to show that theology being implemented and lived out, displaying the men and women who joined ISIS as role models who should be emulated by others.

Not all of these are fighters who seek a path of violence and death. Rather, non-violent religious role models, such as preachers and teachers, caretakers or missionary and media workers are promoted as people involved in a complementary 'peaceful jihad' in pursuit of an 'Islamic State'. Such role models enrich the complex and diverse blend of audio-visual productions emanating from the jihadist movement.

ISIS has learned how best to use non-Arab recruits: in front of cameras, instead of as cannon fodder at the front lines. These individuals tend to address their target audience in their respective languages, and oftentimes they are featured in special videos with

Arabic and non-Arabic titles. This applies to Brits,[27] Germans, Austrians,[28] French,[29] Russians,[30] and so on.

The videos bridge the language gap and serve as a pull factor into the mindset of Sunni extremism. Those who do not speak Arabic and have questions about the Sunni Muslim identity offered by ISIS can find answers themselves by tuning into, for example, English language explanations of concepts like '*shirk*' (polytheism – anything that violates the oneness of God), given by foreign fighters from Cambodia;[31] or they can learn the importance of tearing down the border between Syria and Iraq from a Chilean foreign fighter.

Frequently, non-Arab recruits talk about personal commitment and their motivation for having undertaken the emigration (*hijra*) to the 'Islamic State'. Non-Arabs tend to be keen to explain aspects of jihadist theology in their own language, potentially initiating or drawing their audience into reading magazines such as *Dabiq*, in order to further their education on religious concepts such as "*tawhid*" (monotheism – the 'oneness of God'). Such concepts are absolutely central to the ISIS worldview.

Take the case of Philipp Bergner, from Dinslaken, Germany. He was featured in a video series (no. 32) entitled 'Windows into the Epic Battlefield', showing the very early progress of ISIS in Syria and Iraq in 2013/4. Bergner was a convert who addressed his personal motivations to join ISIS, underlining his commitment to a 'Sunni Muslim identity', while outlining his 'path to God'. Sitting in front of rubble and debris, likely the result of an airstrike, holding a Kalashnikov assault rifle, Bergner introduced himself and asked the viewers to consider who the creator is, and why the human body in its complexity can only be the product of God. Much like the complex and fine-tuned mechanics of a clockwork, he argued:

> this cannot be a coincidence and that is why I became a Muslim. Every prophet was sent by one God[32] – and Islam means submission to the *tawhid* [oneness] of God. That is the translation of Muslim in German. And I am a Muslim. A German Muslim. You too can think about the meaning of life and submit yourself to God as I did.

These words may appear simpleminded, but reflect his attempt to explain what it means to be a Muslim – in the process refuting the Christian tradition of the Trinity, which is considered a violation of the principle of tawhid. Such an explanation would be clear to the overwhelming majority of Sunni Muslims, especially to Arabic native speakers.

27 English is aside from German, French and Russian an important language. Hence the IS magazine "Dabiq" is published in English to ensure a maximum readership worldwide, including the mainstream media outlets. British and American foreign fighters appear from time to time. For example, a video released by Markaz al-Hayyat li-l 'ilam, featuring a British, French and German foreign fighter entitled 'Wait. We are also waiting', 16 October 2014.

28 For example, in a video uploaded from the IS province Wilayat Hims featuring Austrian-Egyptian Muhammad Mahmud and a German by the nom de guerre Abu 'Umar al-Almani. 'Siyahat al-Umma – Der Tourismus dieser Umma', Wilayat Hims, 5 August 2015.

29 For example, the French language nashid 'Tend ta main pour l'allégeance', with English subtitles, Markaz al-Hayyat li-l 'ilam, 24 May 2015.
French is also an important language to reach out to Francophone Muslims. A French speaking Mujahid addressing France threatening future attacks are imminent is concluded by the speaker executing a captured Syrian army soldier in the province of Hama in a video published on 24 July 2015. 'Wa ma zalamnahum wa-lakin kanu anfusahum yuzlamun', Wilayat Hama, 24 July 2015.

30 With a majority of foreign fighters coming from the Caucasus region, IS has a special and Russian-language only media department 'al-Furat' that promotes Russian, mainly Chechen, fighters and ideologues.

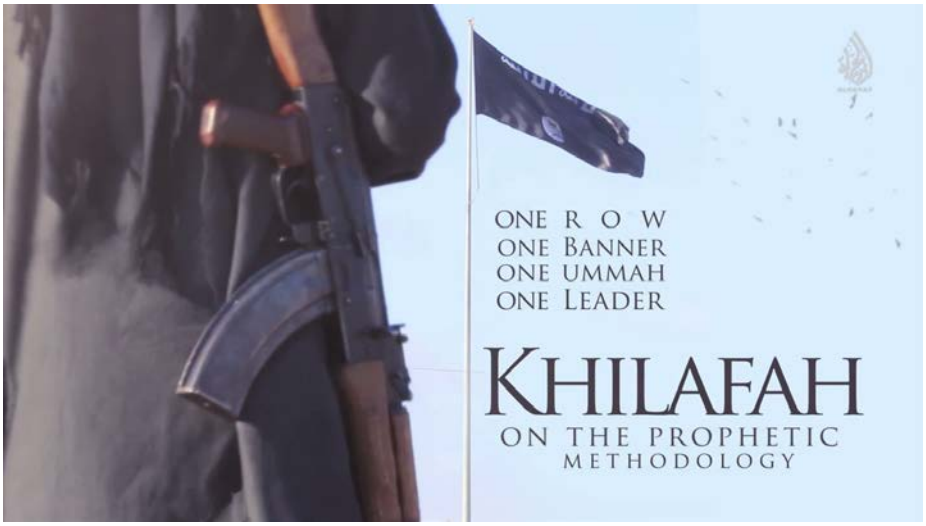
31 'Stories from the Land of the Living – the Story of Abu Khaled the Cambodian from Australia', Markaz al-Hayyat li'-l 'ilam, http://jihadology.net/2015/04/21/al-%E1%B8%A5ayat-media-center-presents-a-new-video-message-from-the-islamic-state-stories-from-the-land-of-the-living-abu-khalid-al-kambudi/.

32 The Arabic subtitles clarify the statement, *bi-tawhid allah*, "by the oneness of God", prophets are dispatched in order to spread the worship to God, Him alone, without partners.

Bergner then continues:

> I migrated to Syria to make the word of my creator the highest. For man-made laws are unjust as we see in this world. Most of the world's resources are in Africa; why are Africans the poorest people in this world? You need to ask yourselves that those politicians in suits are devils who rule by their man made laws and have no interest to satisfy God. They don't even believe in God. They are doing their thing for profit on this earth and we want justice. That is why we are combatting the leaders of the disbelievers and whoever follow them. So that justice and God's law will rule the earth, for God has created this earth and He is the king of kings (...).
>
> All praise be God, I have joined the caravan of jihad as I've said to make the word of God the highest and we are not going to stop until we have achieved this. If we are killed those who come after us will continue to complement the path, for God has promised us this.

The message is clearly stated: fighting for ISIS means being a Muslim. A Muslim can only live within an Islamic *umma* (community); this *umma* can only be considered Islamic if it is governed by *shari'a* law as defined by the jihadists.



As a slogan, the 'caliphate upon the prophetic methodology' encapsulates the goals for which jihadists and their sympathisers struggle. The claim to be imitating the approach of the Prophet is effectively a claim to infallibility. Jihadists justify every action with reference to certain, selectively chosen parts of divine scripture and the prophetic tradition.[33]

33 This concept is outlined further in, Nico Prucha, '*Upon the Prophetic Methodology' and the Media Universe*, Islamic State Briefing, part 2, Onlinejihad.net, http://bit.ly/2w3ZWVm, 1 August 2017.

Dozens of videos glorify every aspect of ISIS activity: the social and civic dimensions of the Islamic 'State', as much as the violent cutting edge. Militants have been portrayed as humanitarians and vice versa. ISIS has understood the importance of making use of the territory it controls and deploys highly able media units in every one of its 'provinces'. These produce videos on a more or less regular basis which aim to show the manifestation and realisation of jihadist creed (*'aqida*) and methodology (*manhaj*). They show variously: 'life in the caliphate'; executions and other sentences of physical punishment (*hudud*), framed as the work of a functioning legal system;[34] the religious policing of communities; the destruction of the shrines of saints; as well as a romantic view on fighting and sacrifice.

Often, these videos are supplemented by theological treatises that justify what is being watched. A good example is provided by one of the many hundreds of ISIS videos showing the amputation of hands:

On the left above is the cover of a 20-page- book that gives the readers a detailed analysis of the divine injunctions to exercise physical punishments against transgressors.[35] The arguments refer exclusively to historical scholars, selected passages from Qur'an and *Sunna*, as well as precedents from history. On the right side are two screenshots from the video 'the ruling of the Creator upon the thief', released by the ISIS province of Nineveh in mid-2015.[36] They show, prior to the act of amputating the two thieves' hands in public, religious references appearing as texts superimposed over the images, to sanction and fully validate this act of punishment according to *shari'a* law. This is the message that ISIS wants to send by its videos: that the 'Islamic State' is based on religious scripture and thus is the only true community of Sunni Muslims; ISIS is therefore acting on behalf of God.

ISIS claims to have restored the *dar al-Islam* (the abode of Islam). It arrogates to itself the right to decide who is a Sunni Muslim and part of

34 See, for one example among many, Nil al-zafr fi iqama al-hudud fi-l ghazu wa-l safr, Maktab al-Buhuth wa-l Dirasa (ed.).

35 Abu Bakr Khalid bin Muhammad al-Shami, Daf'u iham al-tadarruj bi l-tadbiq, Mu'assassat al-Wafa', 2016.

36 Hukm al-khaliq bi haqq al-sariq, wilaya Nineveh, 4 June 2015.

the Sunni community – and who is not. Apostates or traitors are excommunicated (*takfir*) and executed as alleged spies[37] or 'wizards' who conduct black magic[38]; homosexuals are dealt with as 'the people of Lot' and pushed to their death from rooftops.[39]

Left: Announcement and stoning of an adulterer as issued by an "Islamic State court", right: execution of an alleged homosexual, province of al-Khayr, Dhu al-Qa'da 1438 (August 2017).

Less graphically, numerous jihadist videos show children in school settings. The indoctrination of children, taught by self-declared teachers who also fight on the front lines – and who, therefore, fulfil the idealised notion of someone who is both shaykh (knowledgeable in religion) and *mujahid* (fighter) – is an integral part of the long-term strategy of ISIS. By brainwashing children into the extremist mindset, the 'State' seeks to build the next generation of fighters, teachers, police-men and officials – even if its territory is later lost or reclaimed by other groups.

The eighteenth installment of a video series from 2013/4 provided a good example. It took the viewer into a mosque where what appeared to be pre-school children were being taught 'Islamic State' theology – breaking with centuries of local Syrian Islamic values and traditions. The film started with one of the students who gave his name as Abu Shayma' and claimed to have been in the madrassa for more than a month. When asked what he had learned so far, he replied:

> [we learned] *al-'aqida*, *Sunna* and the noble Qur'an. And I learnt a lot about beneficial deeds.[40]

Abu Shayma' then went on to recite 'ten commandments' of Islam from memory, which focused on identifying *shirk* and the '*mushrikin*' (polytheists).

37 For example, Tahalafuhum wa-irhabana, wilayat Nineveh, 20 July 2016 shows the execution of alleged Kurdish spies by French foreign fighters who avenge killed civilians resulting from airstrikes and praise the lone wolf attack in Nice. The attack on Bastille Day by a 'lone wolf' driving a truck into crowds on the Promenade des Anglais resulted in the death of 86 people.

38 La yuflih al-sahir haythu ati, wilayat Barqa, 5 December 2016.

39 'Am 'ala l-fath, wilayat Nineveh, 11 June 2015.

40 A reference to the proper conduct of being a Sunni Muslim and the obligatory prayer rituals that make up this identity. The enforcement of exercising the five prayers gives IS social cohesion and allows to publicly shaming those who do not attend these prayers regularly at public mosques.

Abu Shayma' explaining the tenets of Islam by IS' definition (left); on the right the "study circle"

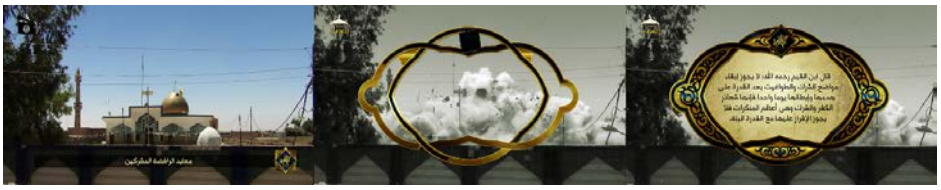
Through videos of this kind, ISIS seeks to frame itself as the authoritative interpreter of Islam – a movement comprised of men steeped in religious knowledge, who are imparting it to the next generation.

By the same token, ISIS underlines its fierce opposition to perceived 'distortions' of the faith and much of its output shows its effort to stamp out heterodox forms of Islam. The Islamic culture of sainthood, for instance, often found within the wider understanding of Sufi Islam and of Islam Nusantara ('East Indies Islam'), is seen by ISIS as a violation of the 'oneness of God' (*tawhid*). To their minds, any anti-*tawhid* manifestation or human behavior must be violently removed to ensure the proper practice of worship to God without distraction. Hence, this culture of sainthood is under attack in Syria, Iraq and elsewhere. The destruction of graves and other sites of veneration by ISIS is a form of consolidating the territory under their control and enforcing the practice of *tawhid* according to their theological parameters. In line with this, a video from November 2013 showed the destruction of a burial site of a saint in the countryside around Aleppo. A caption stated, 'removal of a manifestation of *shirk* and site to worship a grave.'

By destroying a mini-mausolem of this kind, ISIS obliterates the space formerly held by non-Sunni and non-traditional-Sunni Muslims. It is in effect, engaged in a form of genocide, in which the cultural heritage sites, holy places and sites of veneration of their enemies are systematically targeted. This was further illustrated in August 2013, when ISIS bulldozed the 'tree of Moses', which had stood for centuries and was adored by local Sufis. The tree was cut down, its roots dug up and its branches and trunk burned – actions all justified by two speakers who gave a sermon to the locals before the tree was annihilated in this brutal example of *applied theology*.

Bulldozing the "tree of Moses" and sanctioning it as by a historical citation of a companion of Prophet Muhammad

Numerous other videos show ISIS members desecrating graves, smashing historical artefacts and blowing up Shiite mosques on a grand scale, explaining to their audience the theological legality and obligation of their actions.



A Shiite mosque, referred to as "the site of worship for rejectionist-mushrikin" is destroyed; accompanying theological guidance is taken from the works of the historical scholar Ibn al-Qayyum.

Destruction of pre-Islamic mummies in Palmyra in 2016,

Through actions of this kind ISIS presents itself as presiding over the only legitimate zone where Sunni Muslims can properly perform their duties to God. As a statement released in September 2015, at the height of the refuges crisis put it,

> the whole world, from east to west, became *dar al-kufr*, the "abode of the disbelievers". Therefore, God set in motion the establishment of the Islamic State. This state consists of numerous elements that make it *dar al-Islam*. Therefore, the rule of shari'a law returned as well as the implementation of physical punishment (*al-hudud*),[41] cutting off the hands of thieves, punishing adultery by stoning to death and beheading wizards. The establishment of the Islamic State as a reaction to those who commit injustice, governed by "commanding right and forbidding wrong"[42] while driving a jihad against the disbelievers – thus the might of the Islamic community has been restored. Muslims living in the state openly manifest the

41 i.e. the amputation of hand and/or feet as punishment for crimes. This form of jurisdiction is also documented by IS videos to showcase being a functioning state. See iqama hadd 'ala sariqayn, wilayat gharb Ifriqiyya, 2 November 2015.

42 IS has released several documents and videos, sanctioning and showing the destruction of, for example, Shiite mosques, churches, Yazidi shrines, graveyards, or the total obliteration of pre-Islamic statues as well as museums housing these artifacts. "Commanding good and forbidding evil" is the theological legitimacy for the Islamic police, who apart from safeguarding the Sunni integrity by systematically removing sites of veneration that violate the Sunni extremist theology also police communities and, for example, ensure the illicit trade and consumption of tobacco is persecuted. See Nico Prucha, 'Reformatting Space: The Self-Proclaimed "Islamic State's" Strategy of Destroying Cultural Heritage and Committing Genocide', *European Union National Institutes for Culture*, November 2015, http://washington-dc.eunic-online.eu/?q=content/reformatting-space-0.

> rituals of their religion[43], not fearing anything apart from God – therefore the state of Islam is the abode of Islam in this era. It is obligatory for every Muslim to support and protect it, to openly display dissociation and enmity to the enemies of the Islamic State.[44]

This is the essence of the message that ISIS and its sympathisers purvey relentlessly via the internet. It is at the core of the content that they distribute via their online jihad.

Online Jihad – the Swarmcast

As has hopefully become clear, the jihadist movement attaches as much importance to the online space as it does to the physical world. The internet functions as another front (*ribat*) on which they engage – one that often grows in importance as their 'real world' presence is diminished. Hence, prior to 2011, at a time when its influence had been reduced offline, al-Qaeda established a 'jihadist cloud' which, allowed it to remain resilient within 'its virtual spaces and niches on the Internet', irrespective of physical setbacks.[45]

After 2011, the Syrian conflict, now recognised as the most 'socially mediated' in history, developed into the new focal point for jihadi media culture.[46] In this context, jihadist information dissemination evolved rapidly into complex multiplatform systems.

Since 2014, in particular, ISIS has used dispersed forms of network organization and strategy to disseminate rich audio-visual content from the battlefield in near-real time. Its interconnected network constantly reconfigures itself, much like the way a swarm of bees or flock of birds constantly reorganizes in mid-flight. It marks a shift from the broadcast models of communication during conflict, to a new dispersed and resilient form – the user curated 'Swarmcast'. This makes ISIS a challenge for traditionally hierarchical organizations to counter.

2016 started with talk of 'cyberbombs' and transatlantic whispers that ISIS would be wiped off the internet by the end of the year.[47] Almost two years on, it is clear that ISIS maintains a persistent online presence through a mobile-enabled 'swarm' that rapidly reconfigures despite attempts to target key individuals and remove content.[48]

43 Which had been previously banned or could only be taken care of in secrecy under secular Arab regimes to avoid being arrested for possible Islamist oppositional work.

44 Suhayl al-Najdi, Luju' al-Muslimin ila ard al-salibiyyin wa-l iqama fiha, Mu'assasat al-Wafa', September 2015.

45 Nico Prucha, 'Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors', *ORIENT IV* (2011).

46 Lynch, Marc, Deen Freelon, and Sean Aday, 'Syria's socially mediated civil war', *United States Institute of Peace*, 91.1 (2014), pp. 1-35.

47 Richard Forno and Anupam Joshi, 'How U.S. "Cyber Bombs" against Terrorists Really Work', *The Conversation, Scientific American*, 13 May 2016, https://www.scientificamerican.com/article/how-u-s-cyber-bombs-against-terrorists-really-work/.

48 Ali Fisher, How Jihadist Networks Maintain a Persistent Online Presence. *Perspectives on Terrorism*, 9 June 2015, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/426

This 'Swarmcast' is defined by several features:

1) *Speed:*
the ability to rapidly transfer content or information to a wide network of individuals. ISIS and their supporters have successfully executed a netwar-based strategy through which they can distribute video content to a wide network. Over the last 3 years, speed has become increasingly important as social media platforms have increased the rate at which they remove content, which is in breach of their terms of service. This speed of distribution means content removal does not disrupt the network. Instead efforts by platforms to remove content often occur after the media mujahidin have ceased actively sharing it.

2) *Agility:*
the ability to move rapidly between platforms and even adopt new technologies for short periods of time before migrating to other digital locations. This has been an important element which has underpinned the ISIS Swarmcast. The advantage of such agility in maintaining a persistent presence online is that it takes time for the files posted across multiple different platforms to be located – by which time, the content has reached a large network capable of reposting multiple copies, thereby ensuring this content can have a persistent presence online. Further, agility is not merely breadth of platforms, but is also the ability to rapidly adopt new platforms, knowing some will rapidly become obsolete while others flourish.

3) *Resilience*:
the ability to survive takedowns and account suspensions has become an important element of the jihadist Swarmcast. The resilience of the Swarmcast originates from the interconnected nature of the social media accounts and a multiplatform approach to content dissemination. This is a distributed network, rather than being in 'hub and spoke' format, in which one central node facilitates communication between the others. The effect of this is to make it highly resilient and resistant to linear efforts at disruption.[49]

49 Hub and spoke structures have tended to be the result of 'coordination games', where there is a specific strong reason for individuals to huddle around a central node. However, centralised 'hub and spoke' networks can be very fragile, because a loss of the central node, or the strong reason to coordinate around a specific point causes, others in the network to lose contact. This has been long known since simulations run by Paul Baran (published in 1964), showed that "the centralised network is obviously vulnerable as destruction of a single central node destroys communication between the end stations". However, Paul Baran concluded that "extremely survivable networks can be built using a moderately low redundancy of connectivity level ... The redundancy level required to survive even very heavy attacks is not great – on the order of only three or four times that of the minimum span network".

Future policy to counter the dissemination of jihadist content must challenge the Swarmcast on a strategic level. In what follows, we try to explain in greater detail how this network functions, what ISIS is producing, what it means, and how this fits with their overall strategy. We outline the range of content types which are shared and the complexity of the ecosystem through which that content is disseminated. We try to illustrate why disruption has, to-date, not worked, and why claims of decline have been consistently overstated.

To explore these issues, we used data from Telegram, Torrents and other Social Media collected by BlackLight. BlackLight is the data service offered by Human Cognition, based on a genuine collaboration between subject matter expertise and data analysis. This provides access to human-verified jihadist channels and groups run by ISIS, AQ and other jihadist sympathisers. Altogether, this frequently amounts to between 500 and 1000 groups/channels active each week – most of which are in Arabic. The resulting data allows direct and hands on access to the ecosystem of Sunni extremist propaganda and discussions.

Using this BlackLight data we show that ISIS has crafted an effective strategy for producing and disseminating online content to its followers. This process can be broken down into three main stages:

a) **Creation of content** – so as to afford them a persistent online presence
b) **Transmission to the vanguard** – in order to mobilise support, principally via Telegram
c) **Outreach and missionary work** – a multiplatform ecosystem, including mainstream social media sites such as Twitter and Facebook.

Each of these stages will now be explored in turn.

Stage One: Creation of Content

Core content

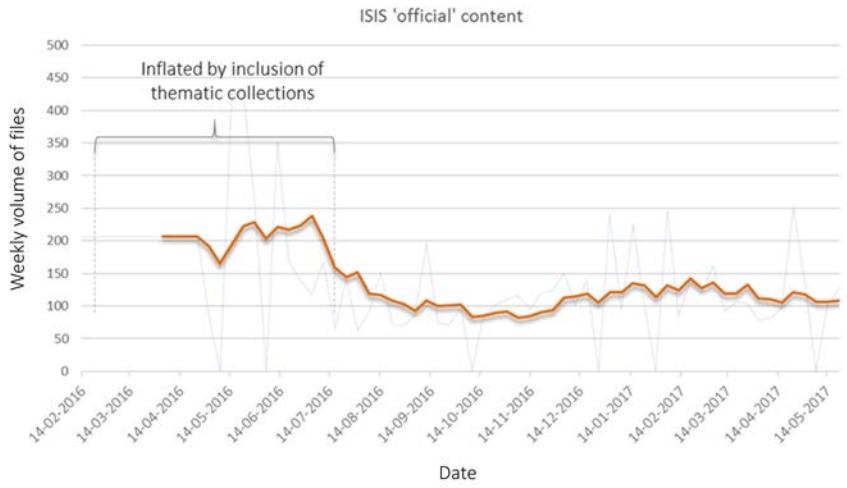
The mix of material produced by ISIS includes weekly core content produced by the *wilayat* (provinces) and media foundations. This is distributed in the first instance, via Telegram, with some of that material then transmitted onto other platforms. As shown in the above section on theology, this contemporary output is underpinned by a massive and continuously growing archive of writings and speeches, which reaches back to the historical roots of the jihadist movement. It is this archive to which the daily content refers, through which theological concepts are explained, and upon which actions are provided with justification.

Analysis of the volume of content can provide a general indication of how jihadist production is evolving over time. Tracking how the level of the narrowly defined 'core' content has fluctuated since the start of 2016, provides context and an overview of the landscape that disruption and content removal is facing. This gives the absolute

minimum amount of new content that needs to be identified each week, in addition to the ever growing back catalogue of content from previous weeks that can reappear.

It is useful to take an overview of current and previous 'core' content production (including the archive of jihadist content, and the array of affiliated content), as this allows one to assess the impact that physical attacks and online disruption have had on the long-term trajectory of ISIS activity online. An overview of this kind provides a strategic perspective and offsets any temptation to speculate on the basis of short-term – even daily – fluctuations in content.

As the graph below demonstrates, ISIS' weekly content production has been largely consistent over the long term, shown by an eight-week rolling mean. For at least a year, the production of content has continued despite the death of key figures, loss of territory and ongoing fighting. As a conservative estimate (below) shows, an average week will require disruption efforts to identify and locate over one hundred new pieces from the ISIS core production.



The graph includes a period of time, shortly after ISIS adopted Telegram as their primary channel of communication, in which content releases included 'thematic' collections. These were collections of documents relating to a specific issue or images and even copies of Western news coverage relating to an attack. As usage of Telegram evolved, the daily content was released separately from thematic collections, causing what might be interpreted as a decline in daily content. In reality, what was happening was the release of different kinds of content through different means.

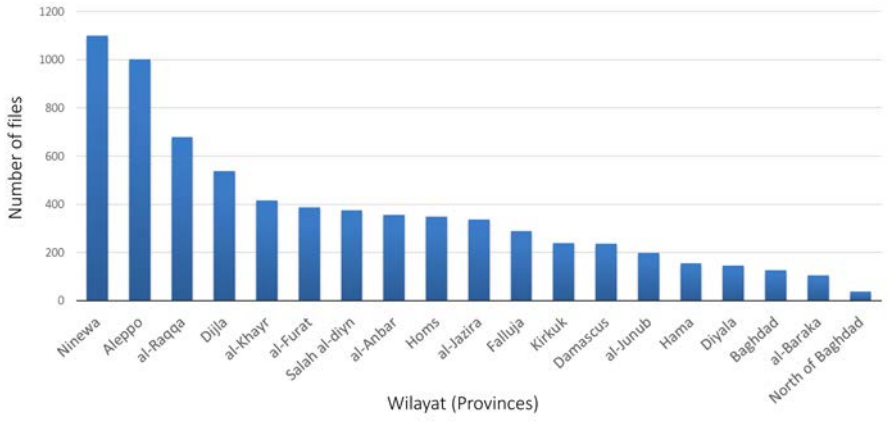
Content of the kind tracked in the above graph can include images, videos, photo reports, newspapers, leaflets, and longform text.[50] In addition, ISIS also produces: almost daily Amaq videos (including from Syria, Iraq, Yemen and the Philippines) and news; al-Bayyan daily radio updates in multiple languages and in both audio and text format; videos from 'affiliated' media houses; thematic collections; and images created by individual users. All of this is augmented by the reposting of older content.

50 In this calculation, a 'photo report' is counted as a single file – rather than as the number of photos it contains. This means the level of content is very conservative, with the actual level of content being higher. Even at this conservative level of production monthly volumes of content are higher than the decline identified in previous studies.

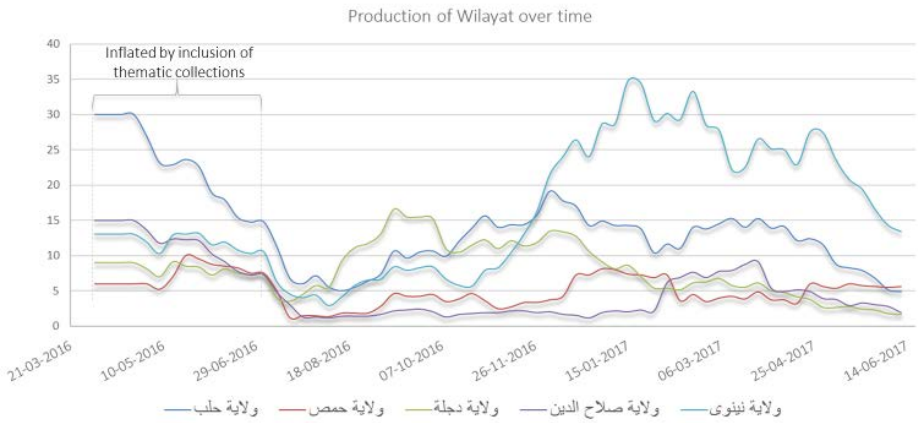
The radio services of al-Bayyan are particularly noteworthy as they give an important impression of what the jihadist ecosystem looks like. Apart from transmitting the daily news (downloadable or streamed as MP3 and PDF text files), the radio station has a large amount of audio files available that range from theological sermons, to tales of the wives of martyrs, or interviews with fighters on why they joined ISIS. Al-Bayyan is reliable, produced daily and reflects the core theological principles that matter most for Sunni extremists.

Content from the 'provinces'

ISIS has divided the geographic areas in which it has a presence into different *wilayat* (provinces) – and these each release region-specific content. The following graph shows the content output of those different provinces:

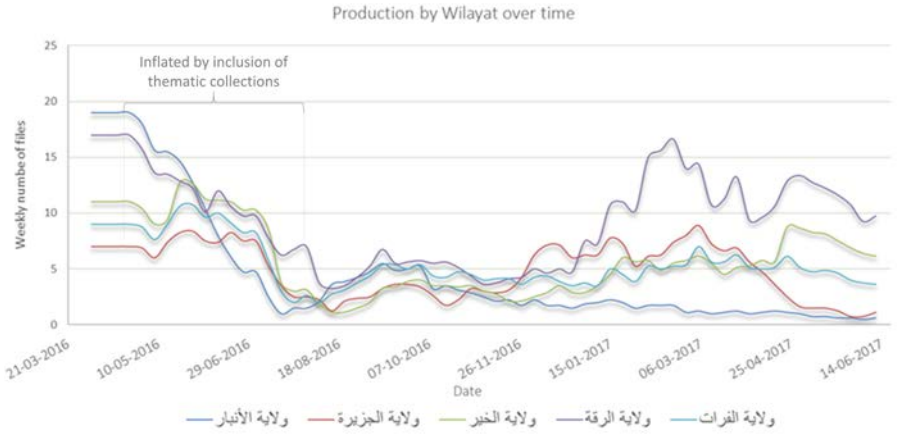


As can be seen, Nineveh province on the far left (which includes the city of Mosul), together with Aleppo, and Raqqa have been the most prominent *wilayat*. However, as the below graph demonstrates, not all *wilayat* were prominent at the same time. It is striking, for instance, that Nineveh became mentioned more frequently in official ISIS releases via Telegram channels/groups once the battle to retake Mosul began in late 2016. Similarly, Raqqa has increasingly become a focal point.



From left to right: wilaya Aleppo, wilaya Homs, wilaya Dijla, wilaya Salah al-Din, wilaya Nineveh.

Other wilayat, meanwhile, such as al-Furat and Homs, are more consistent in their coverage – albeit at a lower level. The fluctuations in content volume from different locations demonstrate the ability of ISIS to modulate the geographic emphasis of content over time, while still producing a relatively consistent output level.



From left to right: wilayat al-Anbar, wilayat al-Jazira, wilayat al-Khayr, wilayat al-Raqqa, wilayat al-Furat.

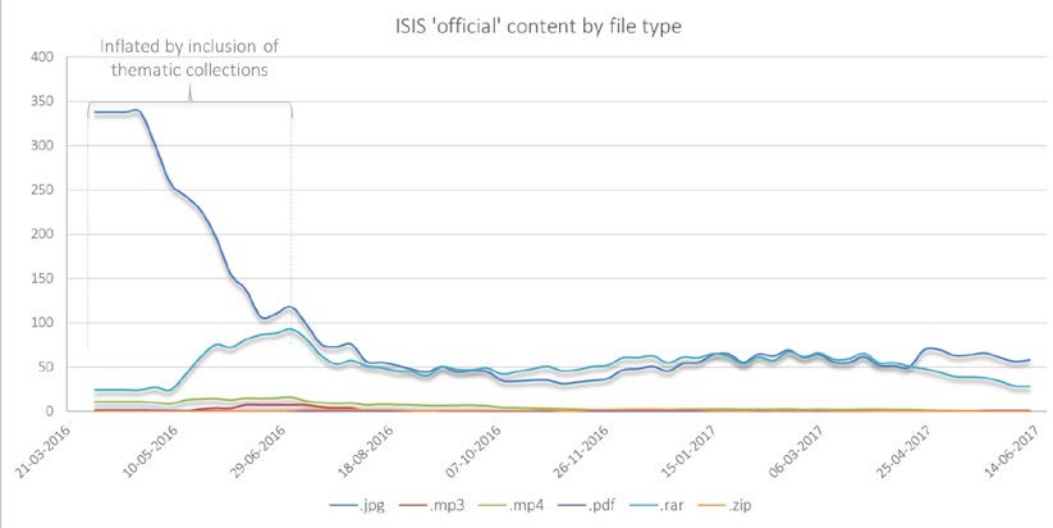
Type of Content

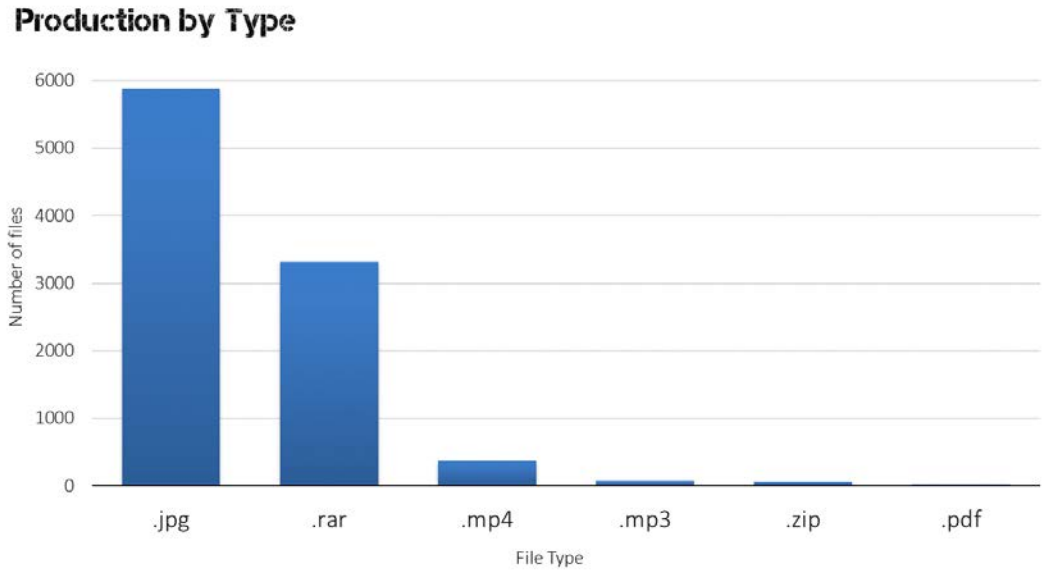
The agility of ISIS – as demonstrated by its ability to continue producing content despite changes in geographic focus – is clear from volume of content from different file types. Once the distortion caused by the initial tendency to distribute thematic and weekly content together is taken into account, the production of content over time remains relatively consistent.

Content production certainly does not show the cliff edge style 30% or 40% reduction in output, which some have claimed.[51] The following graph captures this with a broadly stable level of production from mid-2016 onwards, once the thematic collections were being released separately.

The total production output over the period examined (March 2016 to June 2017) included **5,885 .jpg** images, **374 videos** and **74 audio files** (excluding Amaq and the al-Bayyan daily 'radio' updates). In addition, there were **3,316 .rar files**. RAR (Roshal Archive File) is a means of data compression, which allows larger groups of files to be downloaded more quickly; ISIS use .rar files most frequently for 'photo reports' – a series of images on a particular theme or topic – or distributing other documents in pdf format.

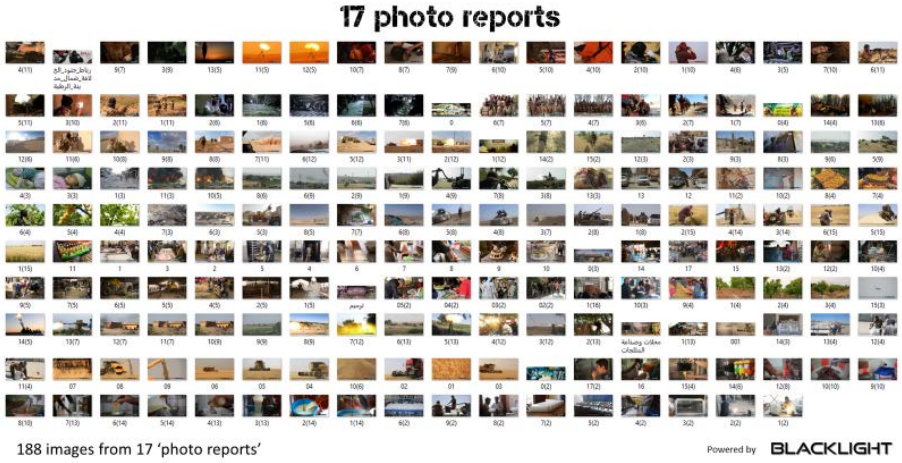
51 Charlie Winter, 'The ISIS Propaganda Decline', ICSR Insight, 23 March 2017, http://icsr.info/2017/03/icsr-insight-isis-propaganda-decline/.





The presence of RAR files is important in developing a closer estimate of the total production level for what we might define narrowly as 'official' content. These files frequently appear on Telegram containing 'photo reports'. Once the user has the report, each image can then be reposted as a separate file, should a user so wish.

Examples from May and June 2017 demonstrate the extent to which this form of content is currently being used by ISIS. For the week ending 29 May 2017, there were 17 photo reports. In total, these reports contained 188 different images.



These images are distinct from the 66 individual photos which also appeared that week, along with: 55 important news items (which appear in the now familiar blue and red colour scheme); 2 videos with associated banners; a Maktabat al-Himma leaflet with two further supporting images; and the weekly issue of *al-Naba'* (the Arabic language newspaper), which contained two high resolution infographic images for easy circulation.

Just combining the individual pictures and images in the photo reports alone produces a total of 254 images. If we add to this the videos, banners, Maktabat al-Himma and *al-Naba'* graphics, then this number rises to over 260 for the week ending 29 May 2017. This is without including the raw battle footage distributed by Amaq. In addition to this core content, al-Wafa' media foundation produced a three page *shari'a*-law analysis and jurisprudential justification of the 22 May attack in Manchester.[52] Based on existing Islamic literature, this fatwa styled document presented the argument why an attack on the British public is not only legitimate but obligatory.

Two weeks later, the week ending 16 June 2017, saw the release of 194 individual images, together with eight photo reports that collectively contained another 104 images. In addition, there was the weekly issue of *al-Naba'* and associated infographic, a banner advertising the new al-Bayyan 'radio' site, and a contribution from the Ajnad Foundation in the form an audio file of a nashid ('My State Baqiyah'), with text and banner image.

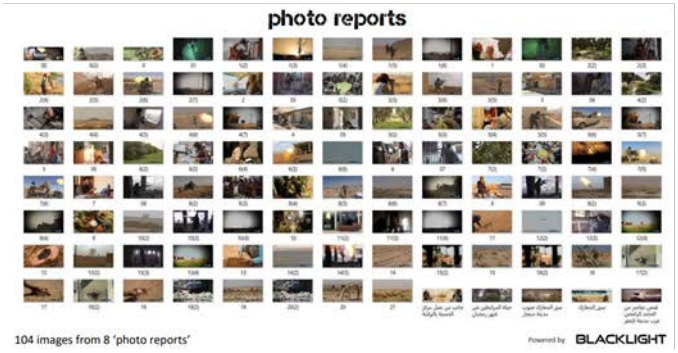
What all of this surely demonstrates is the enduring scale of ISIS' production capacity.

Previous research has argued there has been a 'huge and steady decrease' in Islamic State content.[53] Specific claims include the suggestion that 'the Islamic State's monthly production of visual content dropped from 761 in August 2015, to 194 in August 2016'.[54] **However, both the 2017 *weekly* examples described above, dwarf such estimates of ISIS' *monthly* visual production.**

52 Nico Prucha, 'The Context of the Manchester Bombings in the Words of the "Islamic State" on Telegram', Onlinejihad.net, 27 August 2017.

53 Miron Lakomy, 'Cracks in the Online 'Caliphate': How the Islamic State is Losing Ground in the Battle for Cyberspace', *Perspectives on Terrorism*, Vol. 11, No. 3 (2017).

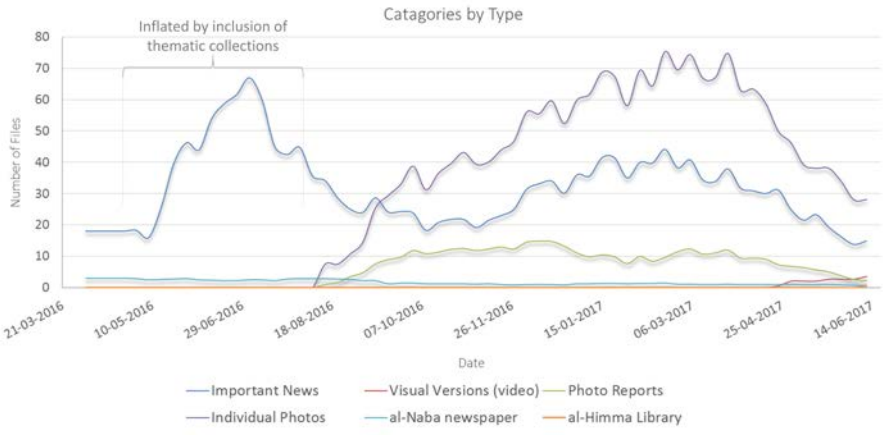
54 Daniel Milton, 'Communication Breakdown: Unravelling the Islamic State's Media Efforts', Combating Terrorism Center at West Point, October 2016, https://www.ctc.usma.edu/v2/wp-content/uploads/2016/10/ISMedia_Online.pdf.



These examples from May and June 2017 show ISIS was capable of producing 260 to 300 visual products in a given week – not months. In addition to this, it produced: a magazine *Rumiyah* (issue 10) available in 11 languages and containing its own mix of imagery; a theological justification of the attack in Manchester; a nashid; videos; and newspapers. And all of this does not include the daily news updates, breaking news and announcements, nor raw footage and news posted by Amaq – nor the vast array of content produced by supporters and aligned (but not officially sanctioned) media groups.

From this evidence, it is clear there has either been a radical turn-around in ISIS' ability to produce content despite the killing of operatives and loss of physical infrastructure, or more likely in our view, there was fairly significant *under sampling* in earlier estimates due to the exclusion of ISIS' core communications channel (Telegram) and weaknesses in methodology.[55]

In addition to tracking production at individual points in time, the BlackLight data also enabled the tracking of fluctuations in content production over time. Analysis shows that the way ISIS has chosen to communicate with its supporters has changed. Changes in content volume are often ascribed to ISIS losing ground on the physical or electronic fronts. However, as the graph below shows, while some formats were in decline, others were increasing.



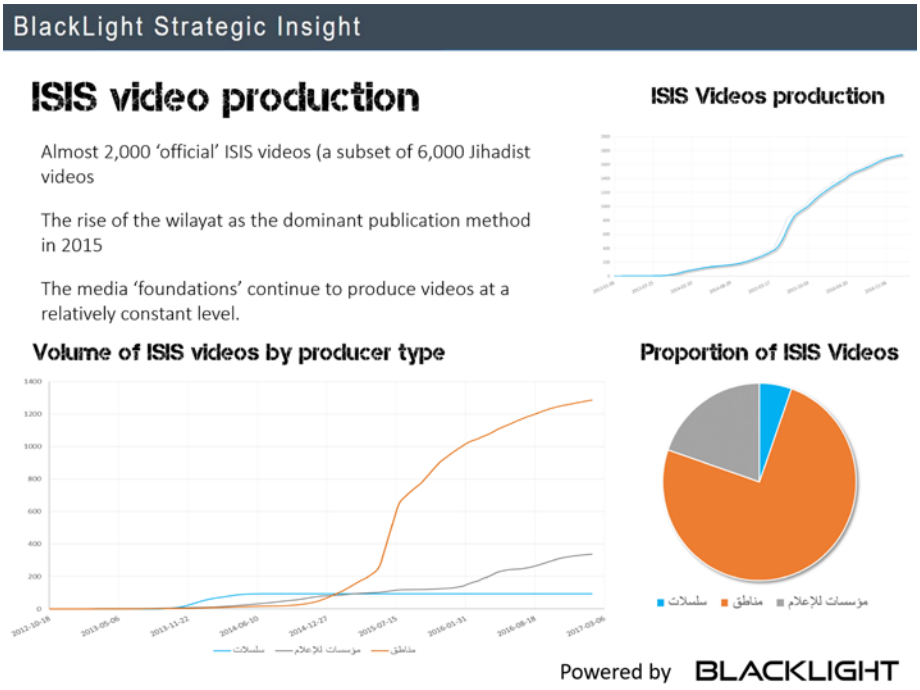
Production in certain periods was lower than others, but it did not show the 'steady decrease' that has been suggested by some commentators. This suggests that ISIS media producers have adopted

55 Ibid., p.40. Also of note, visual products in this report are recorded by type as; video, photo report or Twitter (photo). There are no categories for Facebook (photo), Telegram (photo), nor Torrent files (pp. 22 & 41) which provides a strong indication of the platforms used – and not used – to locate ISIS content. While other studies may have used Telegram their under-estimate of the content volume may speak to challenges locating content or developing a meaningful archiving process for robust data analysis

different methods of communicating their message rather than experiencing a sustained decline.

Jihad on Video

The jihadist movement and particularly ISIS has become particularly well known for video production. ISIS has produced almost 2,000 'official' videos. When those produced by affiliates and the wider jihadist movement are included, this number rises to approximately 6,000 in total.[56]

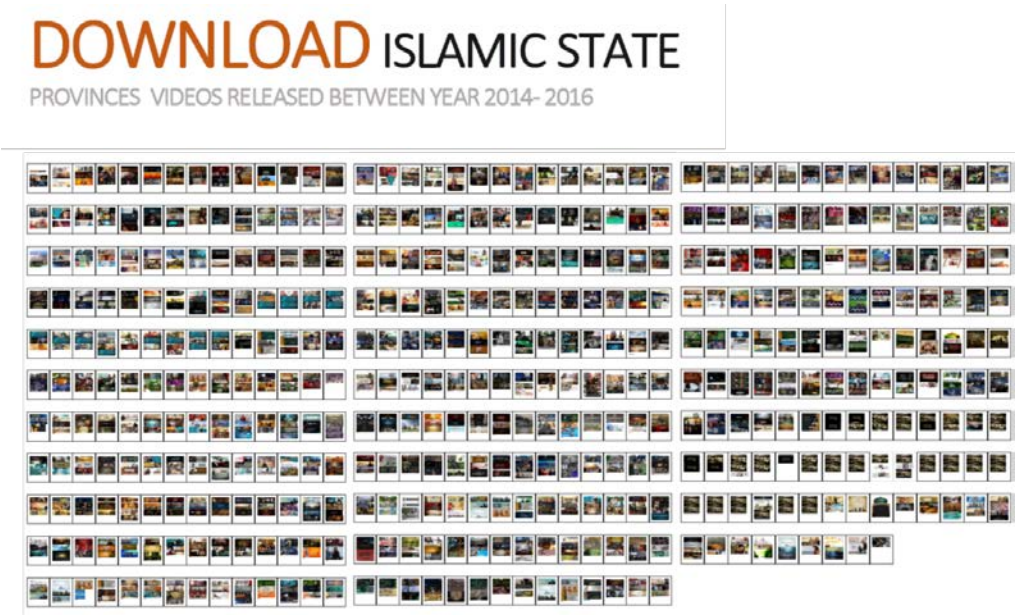


ISIS releases videos that can be categorized by "region" (orange), meaning they originate from a specific wilaya, by "series" (blue) meaning they speak to a particular theme, or by "media foundations" (gray), such as al-Furqan, or al-Hayyat that compiled them.

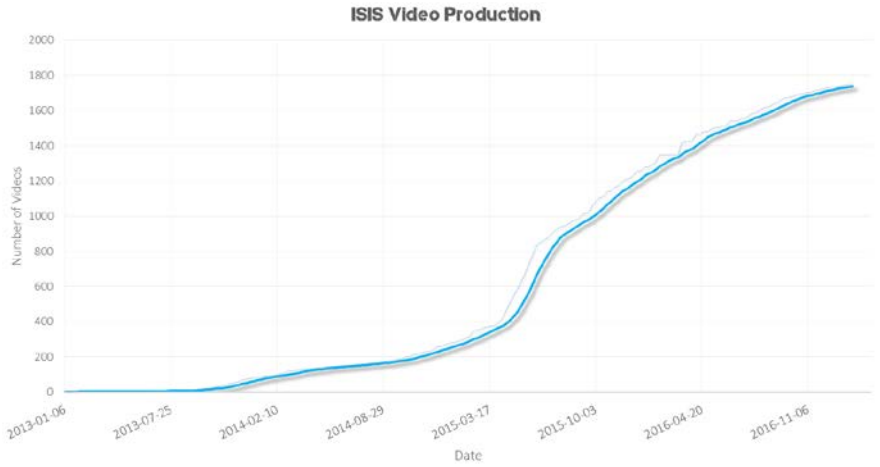
ISIS continues to release videos from various provinces. When a province is lost, for example the wilaya Falluja, then it stands to reason that no new videos are published. However, when ISIS manages to return to contested areas, such as during the fierce battles over the Syrian city of Tadmur (Palmyra), then new videos often spring up, and are included with that specific province.

In the early days when the Islamic State of Iraq swept into Syria, several "series" were released. One key series thematised messages from fighters and men installed to take over local governing positions or manage amenities in Syria – while outlining what ISIS stands for. Another series highlighted the speeches and statements made by AQ senior figures and al-Zarqawi to display that ISIS has succeeded in implementing the very notions for which these men had fought.

56 This does not include raw footage such at that produced by Amaq, individual uploads of combat footage from fighters, and unaffiliated content producers. The latter would include people like Ahmad Musa Jibril, whose videos appear to have played a part in the radicalisation of Khuram Bhutt – one of those behind the London Bridge attacks. The fact that this all exists on top of the ISIS-specific content is a further indication of the vastness of the jihadist ecosystem. Nikita Malik, 'Tech companies must commit to tackling extremism', *The Times*, 3 July 2017, https://www.thetimes.co.uk/article/tech-companies-must-commit-to-tackling-extremism-dmv9kk870.



The approximately 2,000 'official' ISIS videos, as catalogued in the picture above, have appeared at varying rates since 2013.[57] The following graph of video production shows that summer 2015 was an unusually prolific time. This moment coincided with the first anniversary of the Caliphate and Ramadan. However, with this exception, video production has been broadly consistent through to 2017, with multiple videos appearing each week.



It is worth noting that content appeared at a higher rate in 2016 and 2017 than it had during periods of military success for ISIS in 2014 – before the declaration of the Caliphate. These findings challenge another commonly held view – that the volume of production is related to physical world success. It is often suggested that a reduction in content production (compared to a few months in 2015) can be interpreted as a sign of increasing weakness. However, the data shows no correlation of this kind. The pre-Caliphate period, a period of low production, was quickly followed by the greatest series of ISIS military successes to date. Conversely, latter-day military defeats have not

57 The original catalogue was produced by an unknown user in pdf format which included links to all the videos.

produced a collapse in production. To suggest a connection between video production and military strength may make an attractive ad hoc theory, but the data does not support this type of assertion. There are many other factors which influence the volume of production, not least the type of content which made up the video mix.

As shown above, despite occasional drone and air strikes that have killed media operatives, and the on-going challenge of producing high quality videos during a battle, ISIS has continued to produce content.[58] This production has been at a slower rate than at periods during 2015, but they still produce multiple videos each week – in addition to the raw footage produced by Amaq (ISIS News agency).

Stage Two: Transmission to the Vanguard – The Role of Telegram

One critical development since 2015, which highlights the agility of the media mujahidin, has been the adoption of Telegram as a means for ISIS to interact with existing sympathisers. This platform, created by the Russian entrepreneur, Pavel Durov, allows a range of communication options from end-to-end encrypted messaging, to running large group chats, or using 'channels' to broadcast to followers.[59] In 2016, Telegram announced that it had more than 100,000,000 monthly active users. 350,000 new users signed up each day, and as a result Telegram was delivering 15 billion messages daily.

Given that ISIS has codified the use of Telegram as its core communication platform, it must be a core part of any analysis of their online activity. Other platforms such as Twitter, YouTube, and Facebook remain vital for *da'wa* (missionary) type activity and reaching wider audiences. These efforts, however, are coordinated by channels and via groups on Telegram.

As a result, in the clear majority of cases, material is first distributed on Telegram, before then appearing elsewhere. Only a sub-set of content is picked up by ISIS followers and placed on more broad-based social media outlets such as Twitter and Facebook. This means tracking systems and research that are overly reliant on searching Twitter can no longer provide an accurate picture of the content production by jihadist groups, let alone the meaning of that content and the strategy jihadist groups are pursuing.[60]

Why ISIS uses Telegram

What makes Telegram particularly attractive to groups such as ISIS is the combination of security, accessibility, and the range of media features it offers. In addition to being heavily encrypted[61] and allowing messages to self-destruct, users can share an unlimited number of photos, videos and files (doc, zip, mp3, etc.) of up to 1.5 GB each.[62] The service, which syncs automatically across platforms, is accessible via apps for iOS (6 and above), Android (4.0 and up) and Windows

58 'IS confirms death of propaganda chief Abu Mohammed al-Furqan', *BBC News*, 11 October 2016, http://www.bbc.co.uk/news/world-middle-east-37619225.

59 Laith Alkhouri and Alex Kassirer, 'Tech for Jihad: Dissecting Jihadists' Digital Toolbox', Flashpoint, July 2016, p. 7, https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf.

60 For example, a Twitter only study from Maura Conway et al., 'Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts', VOX-Pol, 2017, http://www.voxpol.eu/download/vox-pol_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf.
This report analyses Twitter accounts which are in the vast majority of cases, engaged in Ghazwa. Yet, the report concludes from their analysis that the 'IS Twitter Community is now almost non-existent' (p.46). Given that Ghazwa are coordinated via Telegram, and the focal point of ISIS 'community' has been Telegram for 18 months, the majority of these accounts were never intended to serve a 'community' function. Instead they follow the hit and move approach of classical horse backed raiders. While ISIS strategy was laid out on Telegram, the authors of this report by focusing on the sub-set of content distributed via Twitter misinterprets what ISIS is trying to achieve on Twitter. In so doing, they render their evaluation of the impact of disruption almost entirely pointless as the report is not evaluating ISIS activity against what ISIS is trying to achieve.

61 Telegram FAQs: How secure is Telegram? https://telegram.org/faq#q-how-secure-is-telegram.

62 Telegram FAQs: How is Telegram different from WhatsApp? https://telegram.org/faq#q-how-is-telegram-different-from-whatsapp.

Phone as well as via a web version or desktop apps for Windows, OSX, and Linux.[63] In addition, across devices, users can move easily from watching a video, to listening to audio, to participating in large group chats, to one-to-one text chats, and to making voice calls.

The way Telegram treats user data makes the system particularly secure. If an account holder uses a 'secret chat', it is protected by end-to-end encryption, and Telegram has no data to disclose to third parties or government agencies. Telegram further states:

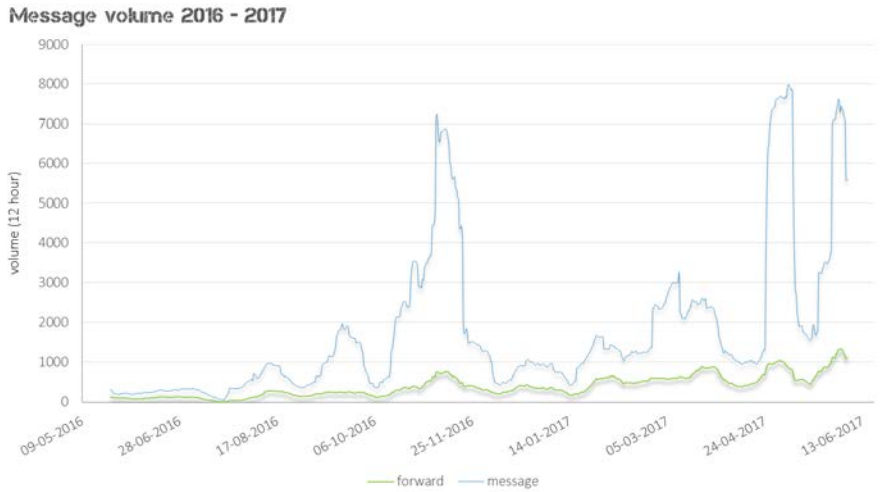
> To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.
>
> Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.
>
> To this day, we have disclosed 0 bytes of user data to third parties, including governments.
>
> While there has been much commentary and speculation about content removal and account suspension, Telegram states:
>
> All Telegram chats and group chats are private amongst their participants. We do not process any requests related to them. But sticker sets, channels, and bots on Telegram are publicly available. If you find sticker sets or bots on Telegram that you think are illegal, please ping us at abuse@telegram.org.[64]

The combination of security and user experience makes Telegram an attractive and powerful communication tool for the jihadist movement. The security makes it a safe haven from which to coordinate online activity including 'raids' (*ghazwa*) onto other social media platforms, while the user experience makes it an ideal locus for galvanising core supporters, the mujahid vanguard.

Telegram has been a core part of the jihadist information ecosystem for around eighteen months. The following graph shows the fluctuation in the content posted within jihadist channels and groups on Telegram.

63 Telegram FAQs: Which devices can I use? https://telegram.org/faq#q-which-devices-can-i-use.

64 Telegram FAQs: There's illegal content on Telegram. How do I take it down? https://telegram.org/faq#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down.



Over the last year, *BlackLight* collected over 1,300,000 Telegram posts from channels and groups operated by members of the jihadist movement, primarily ISIS. Of these posts, over 300,000 were 'reposted content' messages i.e. they were messages that had been posted by one channel, that were then reposted (like a retweet) by a channel known to be operated by a jihadist. The significance of this 'reposted content' is that it represents the content, which the core of the movement is particularly trying to promote.

Engagement with these channels is significant. A channel representing the Jihadi media foundation al-Wafa' has over 31,000 followers, while another produced by Jabhat Fatah al-Sham (JFS, previously known as Jabhat al-Nusra, or the Nusra Front) has more than 22,000 followers.[65] The forwarding of content posted by pro-ISIS channels into other channels currently runs at around 2,000 posts per day with a bias toward daytime in the Middle East and Europe.[66] This 'heart beat' of the movement has been largely unaffected by disruption from channel suspensions and the killing of media operatives in drone strikes. Instead it has displayed a slow but steady growth over the last 12 months. (It should be noted that the total number of messages collected in a given period, fluctuates wildly – often due to pro-Shiite accounts penetrating ISIS groups to flood them with anti-ISIS content. However, the sharing of content between verified ISIS channels has remained broadly constant, whilst showing a slow increase in volume overtime.)

Telegram plays host to a rich array of audio-visual content promoting the jihadist message. Shown below are all the images shared by a single Telegram channel focused on Mosul between February and June 2017 (approximately 2,700 images).

65 Follower numbers accurate 27 February 2017.

66 This number represents only that content forwarded by a human verified ISIS channel, which was originally posted on another channel. This does not include the vast ecosystem of pro-ISIS groups or chats which also exist on Telegram.

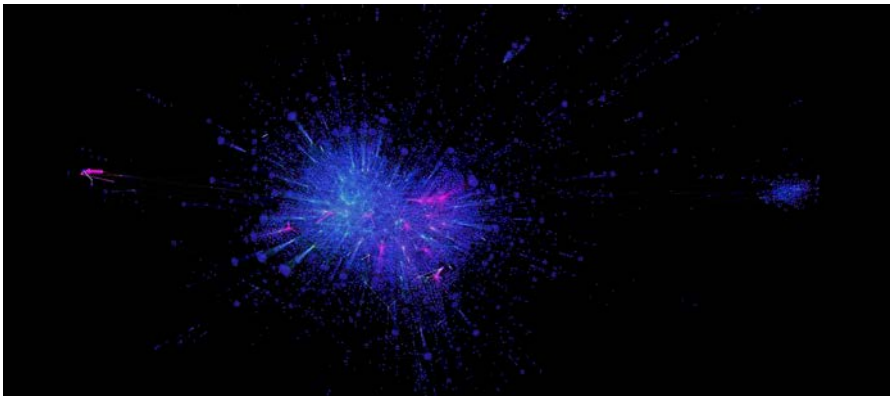
In short, Telegram acts as the core of the jihadist movement online. ISIS channels and groups distribute vast archives of content, direct raids to other platforms and provide a safe haven where users can find the latest releases before posting them elsewhere. In addition, groups provide the means for users to connect and discuss possibilities for taking action – whether that means finding a way to join ISIS (performing the *hijra*) or learning how to make bombs or poisons.

A Resilient Network - the Swarm

Telegram, simply by virtue of its technical structure, provides a degree of resilience for the jihadist movement. However, a further source of resilience for the 'media mujahidin' is the network structure that they themselves have developed to distribute content and maintain a persistent presence in the face of disruption. This structure was previously identified on Twitter but has now also been adopted on other platforms.[67]

Taking the afore-mentioned 300,000 messages of 'reposted content' as a start-point, it is possible to construct a directed network graph of ISIS activity on Telegram. This shows there were more than 8,900 channels active in the last year. 97% of these channels were all connected into a single 'giant' network component, which also includes 99% of all the edges (links between channels). The remaining 3% of channels were scattered across 100 smaller components. This is represented figuratively below.

67 Ali Fisher, 'How Jihadist Networks Maintain a Persistent Online Presence', *Perspectives on Terrorism*, Vol. 9, No. 3 (2015), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/426/html.



Analysis of the ISIS network shows that there were a small number of channels which primarily posted original content; this was then reposted by other channels. The top 10 most shared channels were collectively reposted 17,355 times. In addition, there were a larger number of channels which primarily, or solely reposted or aggregated content. The top ten channels most actively reposting content collectively shared 23,715 posts.

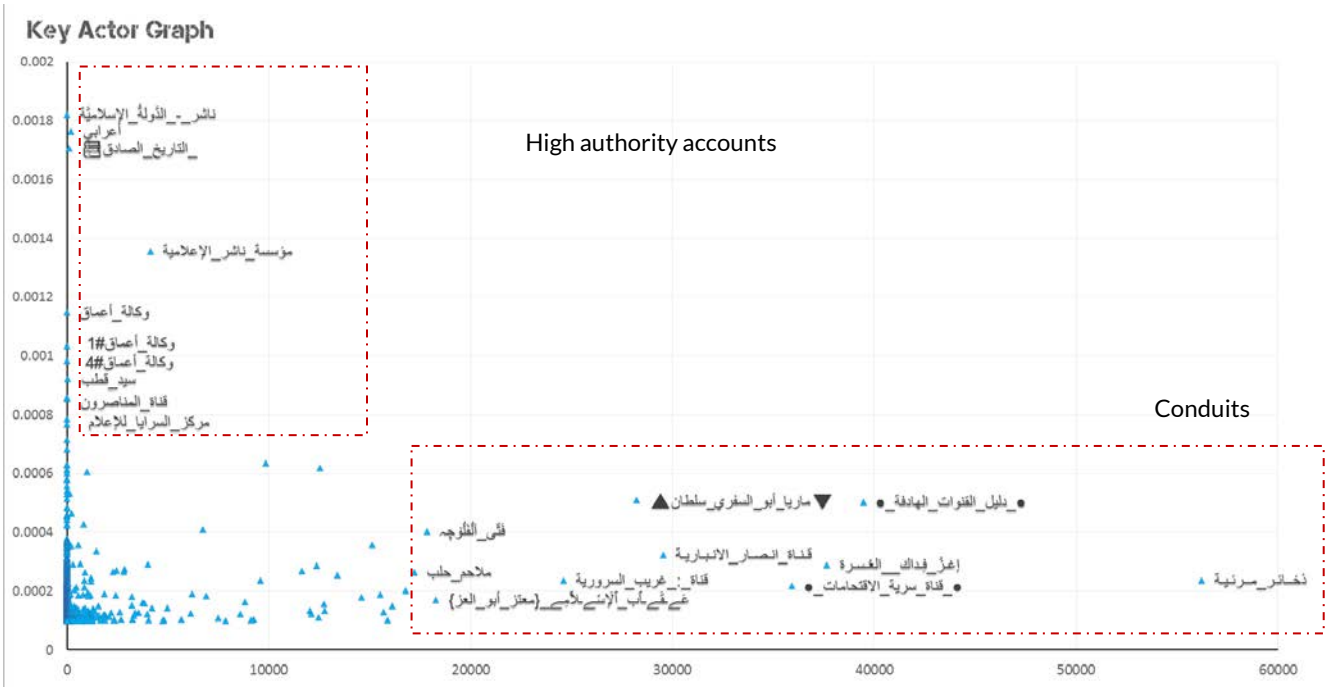
All of this provides a level of resilience within the Swarmcast. If the original channel is removed, users can still find the content on the channels that reposted it. Likewise, users can reconnect with the new version of the channel when it resurfaces, as the existence of such channels are often announced via reposts that include an 'invite link' (a time limited link which is required for a user to join the channel). Conversely, if the channels aggregating content are removed, users will have already had the opportunity to connect with some of the channels that originally posted content, or other channels which aggregate content.

Network metrics confirm this. While the network has a diameter of 19 (the number of connections between the two most distantly connected nodes) the average is a little over 5 connections between two nodes.[68] This is not dissimilar to the 'Six degrees of Separation' investigated through the small world problem, and later by Facebook research.[69] What this means in short, is that users accessing ISIS content on Telegram are rarely far removed from numerous other sources of this content. Users are able to rapidly grow the network of channels they follow, meaning the loss of a few has little impact on the overall experience.

A key actor graph, generated from the giant component of the network, further demonstrates the way in which different accounts within the ISIS system play different roles.

68 For more on calculating network diameter see Douglas B. West *Introduction to graph theory*, (Upper Saddle River: Prentice hall, 2001) (2nd edition) and Fan R.K. Chung, 'Diameters of Graphs: Old Problems New Results', *Congressus Numerantium* (1987), pp. 296-317, http://www.math.ucsd.edu/~fan/mypaps/fanpap/107diameters.pdf.

69 Jeffrey Travers and Stanley Milgram, 'An experimental study of the small world problem', *Sociometry* (1969), pp.425-443; Jeffrey Travers and Stanley Milgram, 'The small world problem', *Phychology Today* 1 (1967), pp. 61-67; Edunov, Sergey, et al., 'Three and a half degrees of separation', *Research at Facebook* (2016), https://research.fb.com/three-and-a-half-degrees-of-separation/.



The above Key Actor Graph plots 'PageRank' against 'betweenness'. Those who are particularly authoritative within the network tend to have a high PageRank score. Conversely, those with a high 'betweenness' score tend to be conduits for information to flow between different parts of the network; they are often responsible for distributing information from the core of the network to a wider audience.[70]

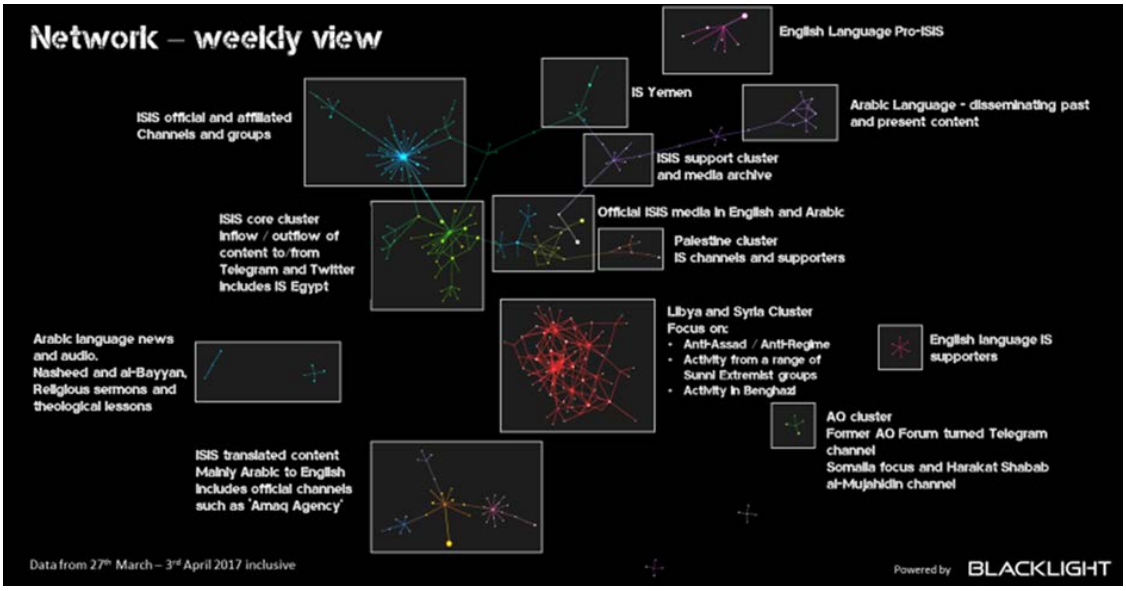
In sum, what all of this underlines is the extent to which different channels play different roles within the network; and therefore, the disruption of some Telegram Channels does not disrupt the network as a whole. Instead, the ISIS ecosystem continues to share content.

The graph representing over a year's worth of activity can appear an impossibly complex hairball. However, when viewed as separate weekly networks, the habits of sharing between specific channels highlights their collective focus. This allows them to be identified through their collective efforts, rather than as individual and separate channels.

One crucial consequence of understanding this, would be to help efforts at information disruption move on from existing 'whack-a-mole' approaches, to become far more strategic about the clusters of channels that are targeted. Equally, when understood as a network, the relational dynamics between the remaining channels can be assessed to analyse how channels are responding to disruption.

The ability to identify clusters of accounts is shown in the graph (below) from a single week in March – April 2017. It shows how different clusters focus on different locations, and how some clusters perform specific functions including disseminating official statements, sharing translations, or distributing content from the jihadist archive.

70 O'Flynn Peter and Chris Barnett, 'Gauging Demand for Evidence and Accountability in Impact Investing by using Twitter Social Network Analysis: A Methodology', Institute of Development Studies Evidence Report 213, November 2016, http://www.ids.ac.uk/publication/gauging-demand-for-evidence-and-accountability-in-impact-investing-by-using-twitter-social-network-analysis-a-methodology; Alistair Willis, Ali Fisher and Ilia Lvov, 'Mapping networks of influence: tracking Twitter conversations through time and space', *Participations: Journal of Audience & Reception Studies* 12.1 (2015), pp. 494-530; Drew Conway, 'Social network analysis in R", Revolutions, 17 August 2009, http://blog.revolutionanalytics.com/2009/08/social-network-analysis-in-r.html.



Stage Three: Outreach and Missionary Work

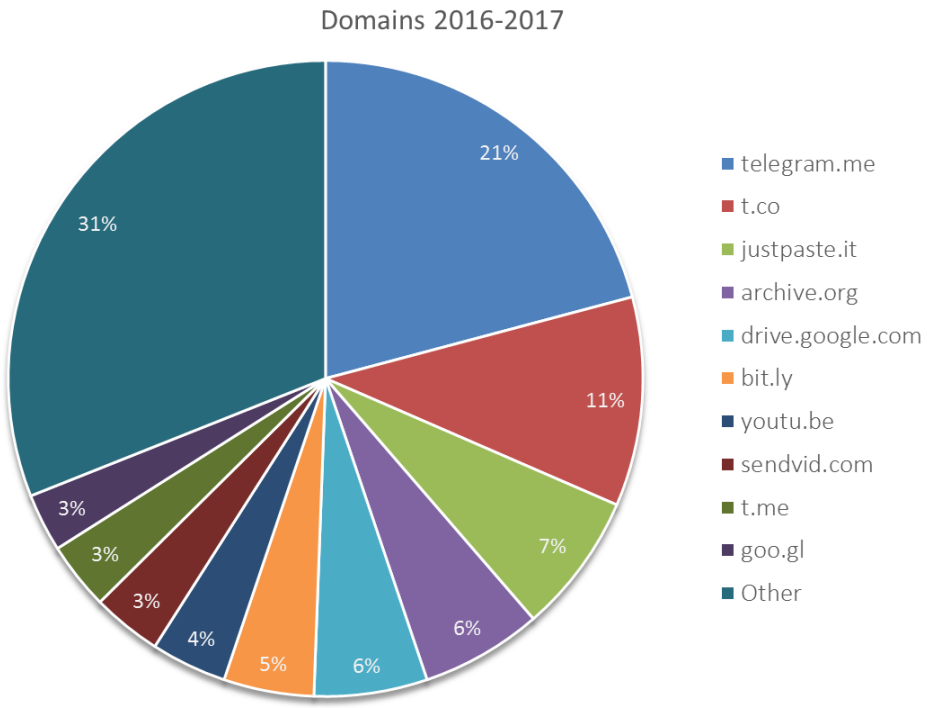
Content Sharing

While Telegram is currently an important platform for the jihadist movement, it is just one of many in their information ecosystem. To provide a conservative estimate of the number of other platforms that ISIS core members are using to distribute content, we identified and analysed all the shared URL (i.e. web addresses) contained in the 300,000 reposts discussed previously. This sample of 300,000 reposts was used, because it represents the 'important' or 'authoritative' content that is disseminated from the core of the movement. The results show which other platforms and distribution methods the jihadist movement is using.

The 300,000 messages contained 21,585 unique URL, which collectively were reposted a total of 35,668 times. This means approximately 11% or 1 in 9 messages contain a link to the source of further content. On average that equates to almost 1800 individual URL a month, even before any reposting by 'outsiders' is considered.[71]

Analysis of where these URL lead the user demonstrates the breadth of the ecosystem and the other prominent platforms within it. As the below chart shows, just under a quarter of the URL (24%) connect the user to further content on Telegram, usually through invitations to join new groups or channels.

71 This is a consciously conservative estimate, it excludes links posted in a verified Jihadist channel which were, for whatever reason, not reposted. It also excludes links shared in group discussion, which can include requests for specific content. As with the estimate of content production, this should be considered the minimum level.



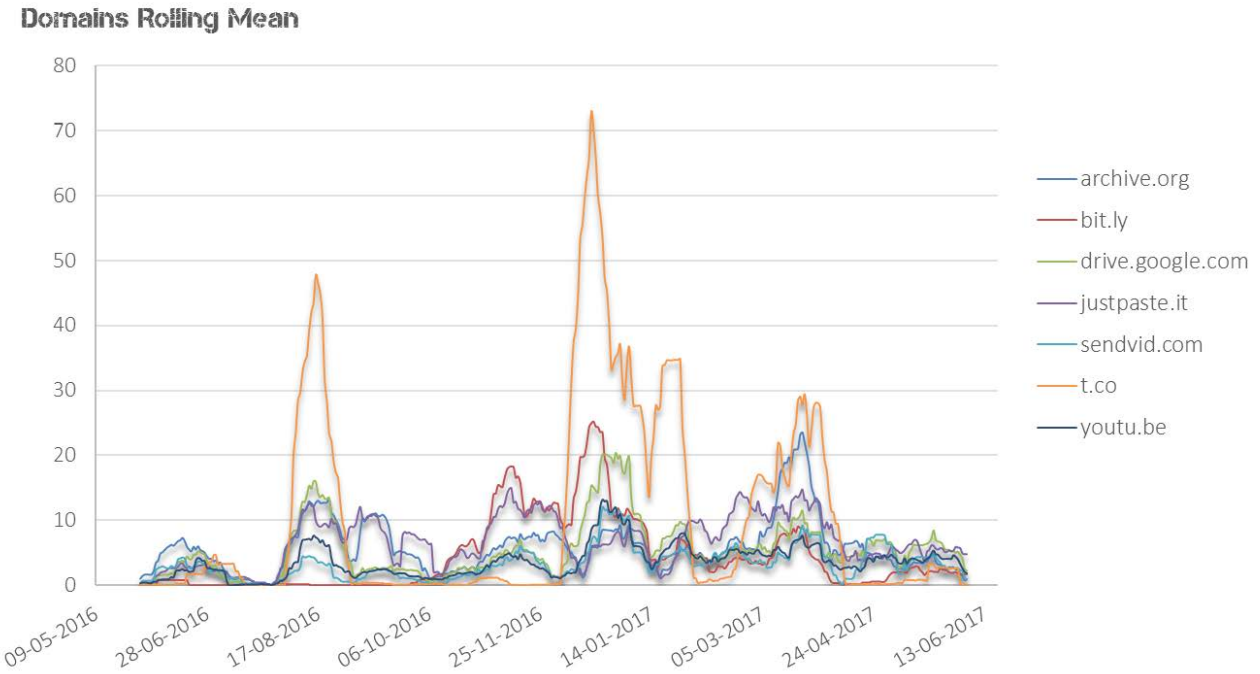
Yet what analysis of the distinct URL clearly demonstrates is that while Telegram is a 'safe haven', the jihadist movement has not abandoned using other platforms. Instead the information ecosystem is a dynamic multiplatform zeitgeist.

76% of the total shared by verified jihadist channels over the last year, lead users to locations outside Telegram which are familiar to most frequent users of the internet. These are the forums used by ISIS to reach out to a wider audience; collectively they are the site of the group's missionary work (what it calls its *da'wa*). The effect of this is that content is spread across the web in a vast information ecosystem rather than a few vulnerable platforms.

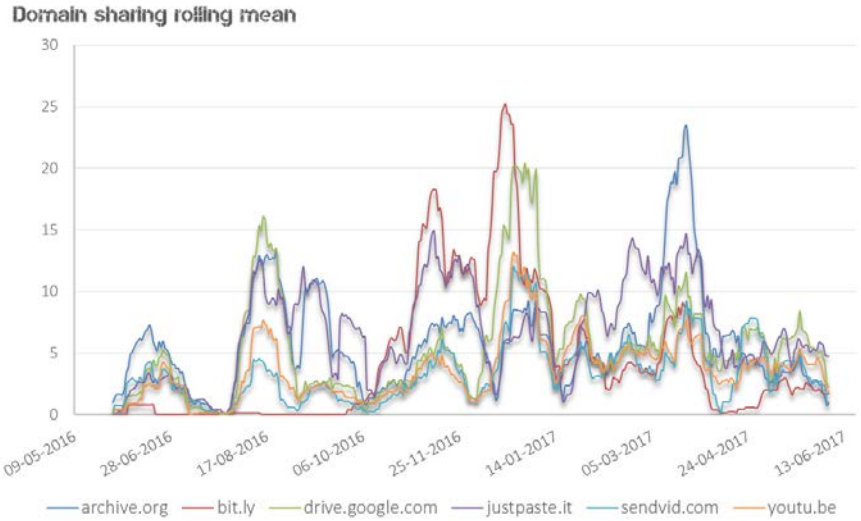
In total, if subdomains are counted as distinct entities (such as different blogs using ###.wordpress.com) there are over 400 distinct domains. The 8 most frequent specific domains, which are not Telegram, represent 45% of all URL shared by core ISIS channels, the largest proportion of which are t.co (Twitter) at 11%.

In itself this might not seem like an especially large figure. The same could be said of Facebook, which accounts for just 4%, while Google Drive and archive.org each feature 6% of the time respectively. Yet what matters here is the way in which these small proportions coalesce into a flourishing, cohesive ecosystem. The removal of any individual part will scarcely solve the problem. As such, pressure on an individual platform to act will have little impact on the ecosystem. **It is the ability to target the strategically important parts of the network collectively where large-scale inroads may be possible.**

As the next set of graphs demonstrate, the use of these different domains fluctuates over time. This presents further problems for those charged with attempting to disrupt the jihadist movement and in measuring the impact of that disruption. The shift from a constant presence on Twitter to raids coordinated from Telegram, leads to sharp spikes in sharing of t.co links.



In addition, some Telegram groups coordinated by ISIS supporters monitor news coverage about the jihadist movement. They provide commentary on journalists reporting on attacks; and they highlight what academics are saying about the jihadist movement. As these massive spikes can obscure other domains, the graph below with figures for t.co (Twitter content) removed shows with greater clarity the fluctuation in the use of some other platforms.

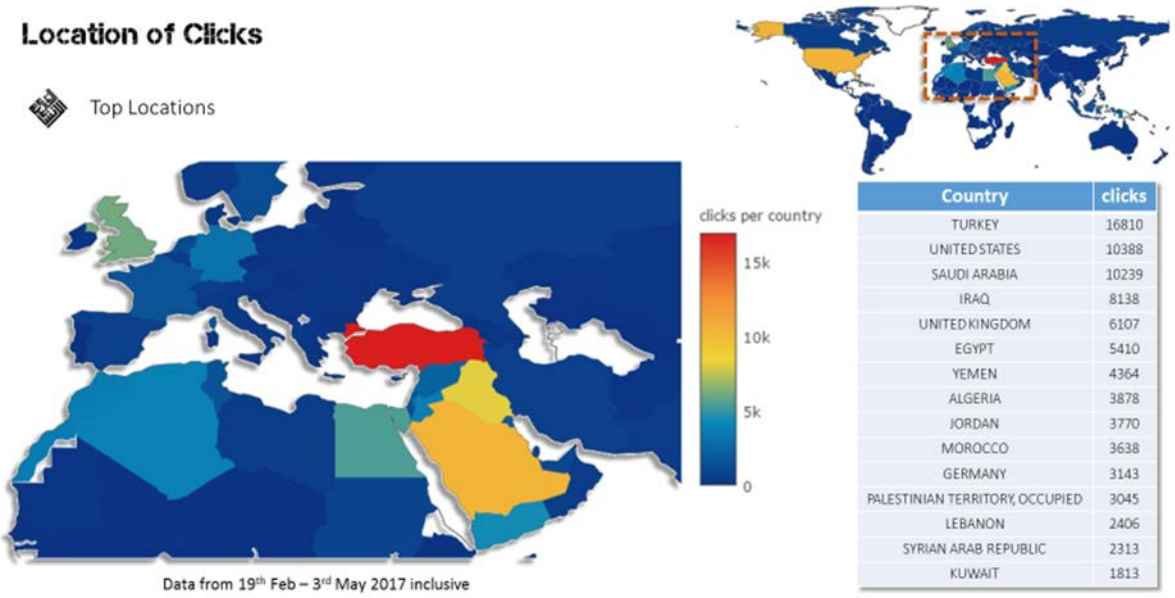


As can be seen, the use of Bit.ly (often associated with the sharing of amaq content) was particularly prominent in the first months of the battle to retake Mosul from late 2016. At different points, Archive.org and Google Drive were especially important locations for storing videos, with YouTube and Sendvid used at a more constant rate. Even this relatively narrow range of platforms for sharing content, within the much wider ecosystem, creates a level of redundancy which makes it easier for supporters to access content even when some versions have been removed.

Where are Users Accessing Content?

Links to content are sometimes shared using 'shortlinks'. Shortlinks are provided by services such as goo.gl or bit.ly, that take a long URL and create a shortened version to make sharing easier. One of the services which shortlinks providers offer is aggregated data on the countries from which users click on the link. This provides, with some caveats, a rough view of how many times a link was clicked in each country.[72] As the following graph shows, in the period between mid-February and early May 2017, Turkey was the location with the most clicks overall, followed by the US, Saudi Arabia and Iraq. **The UK was the fifth most frequent source of clicks, and the most frequently identified source of clicks for a European country.**

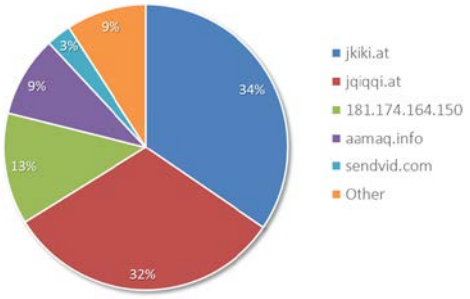
72 Some users will have adopted methods of obscuring their location, but many will not. Equally figures are shown as absolute rather than proportionate to the size of the population.



Country	clicks
TURKEY	16810
UNITED STATES	10388
SAUDI ARABIA	10239
IRAQ	8138
UNITED KINGDOM	6107
EGYPT	5410
YEMEN	4364
ALGERIA	3878
JORDAN	3770
MOROCCO	3638
GERMANY	3143
PALESTINIAN TERRITORY, OCCUPIED	3045
LEBANON	2406
SYRIAN ARAB REPUBLIC	2313
KUWAIT	1813

In addition to location, shortlink providers show how often each individual link was clicked. As the following table and chart reflect, the most clicked link was a shortlink disguising access to a Telegram Channel.

clicks	Long URL
21296	https://telegram.me/ha****
2236	https://jkiki.at/2017/03/15/تقرير-مرئي-القوات-العراقية-تخسر-17-ألية/
1988	https://jkiki.at/2017/03/21/تقرير-مرئي-1800-قتيل-من-أهالي-الموصل-ضحايا/
1638	https://jkiki.at/2017/03/11/الموصل-آثار-القصف-الأمريكي-بالفوسفور/
1564	https://jkiki.at/2017/03/13/خسائر-بشرية-لقوات-النظام-مع-استئناف-مع/



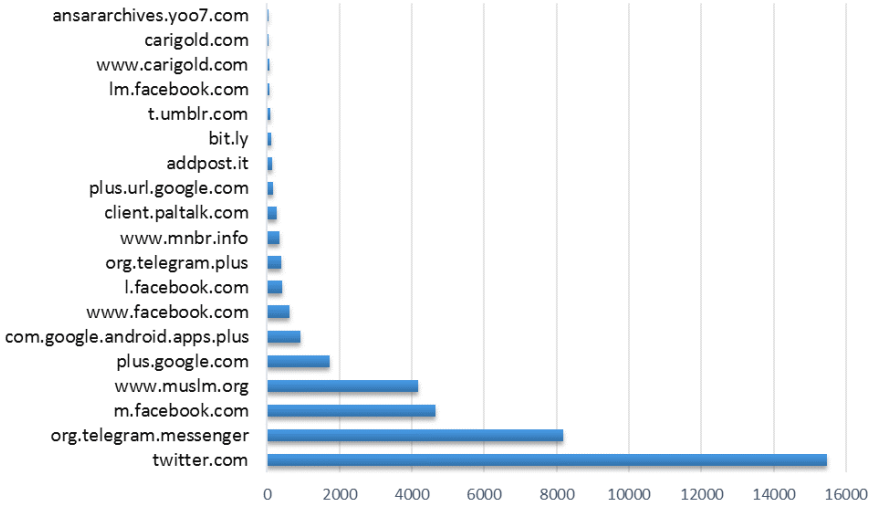
Other than this, top links were predominantly directing users to Amaq content that was hosted on domains known to aggregate ISIS content. This highlights another element of the ecosystem: that a single shortlink URL shared via Telegram and subsequently on other platforms allows users to access content aggregators, which display a whole range of Amaq 'news' content.

Beyond purpose built aggregators of Amaq content, the most common target domain was Sendvid which is often used to post short clips of 'raw' Amaq footage.

Referrers

The shortlinks data also provide an indication of the platform from which users access content. This allows us to see where the audience for ISIS content is located, which provides a vital perspective on how information is dispersed through the ecosystem. For the links made available via ISIS Telegram channels, 65% of them are recorded as 'direct'. This means the user either pasted the link directly into a web

browser, or the shortlink providers were unable to detect a referrer. However, for those clicks where the referring platform was detectable, the results are telling. The graph below highlights the breadth of the ecosystem and the platforms pointing users to this content.[73]



Of the clicks for which there is a known referrer, 40% are from Twitter, followed by one of the Telegram messenger apps and Facebook for mobile. This is vital to understanding how the ecosystem works in its entirety. What it demonstrates is that, although ISIS communicates with the *mujahid* vanguard on Telegram, it still conducts a large amount of outreach (*da'wa*) via more mainstream platforms such as Twitter, Facebook and Google.

Furthermore, this data again contradicts the narrative of decline and specifically the purported degradation of ISIS distribution on Twitter.[74] The data shows that there is a wide range of platforms driving traffic to this content, but that Twitter is a key and in many ways dominant means of delivering content to those not already accessing it via Telegram. Twitter, in other words, is a crucial gateway to the uninitiated – to those ISIS most hopes to target via its outreach.

A recent UK Home Office-funded research project produced by VOX-Pol concluded that 'the IS Twitter community is now almost non-existent' and 'this means that radicalisation, recruitment and attack planning opportunities on this platform have probably also decreased'.[75] Yet, as we have demonstrated, the dominance of Twitter within the click-through-data suggests that these researchers were simply unable to locate the content being distributed – rather than the absence of ISIS' use of Twitter.

To conclude this section, what is clear is that the jihadist ecosystem, the core of which is rooted in Telegram, has tentacles that spread out across hundreds of different domains. It is resilient and reaches an audience of, at minimum, tens of thousands, including large numbers of users in the UK. That reach is magnified by the wider information environment in which it exists and the ease with which ISIS content is found. It is to that issue that we turn next, noting that one of the

73 The referrers data has been left as it is delivered from the shortlink services rather than combining all numbers for a single platform. This is because platform providers use different domains and subdomains to denote different parts of their service and this research seeks to maintain that nuance.

74 Maura Conway et al., 'Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts', VOX-Pol, 2017.

75 Ibid., p.45.

unfortunate features of the jihadist network is the way in which it is being inadvertently facilitated by those who stand opposed to it.

The Information Environment – the Problem of 'Findability'

The importance of 'findability' (ensuring your content is easy to find) has been an underpinning concept of online marketing since the beginning of the mass use of the internet and is as important to jihadist groups as it is for any other organisation in the twenty-first century.[76] The information environment in which ISIS operates has changed since 2014. This section of the report shows that despite efforts at disruption and content removal, jihadist content remains 'findable'. Unfortunately, it is clear that the actions of some news media, intelligence analysis companies and academics have undermined the efforts of disruption / content removal and increased the scale of the audience that ISIS has been able to achieve.

News organisations such as the BBC, whose international television news services reach 162 million viewers, now show sections of Amaq videos.[77] Equally, the Mail Online, which has 240 million monthly global visitors, features sections of videos from ISIS production houses such as al-Furqan and various *wilayat* including Ninawa.[78] Fox News featured the full unedited, non-commented ISIS video showing the execution of the Jordanian pilot Mu'adh al-Kassassiba, giving the extremists another platform to share this particular video.[79] The broadcast and streaming of this content in this way, significantly broadens the reach of ISIS content beyond that which it alone could achieve for its content.

Beyond this, the behaviour of researchers and commercial organisations provide new gateways for the curious to locate jihadist content (and for core members to revisit content), by making it more easily 'findable'. This comes in the form of directly sharing content through links, providing the names and announcements of new content, or images that can be used to find the original pdf versions for download.

One way in which jihadist content becomes increasingly 'findable' is following an attack, such as that on Westminster Bridge (March 2017), or Manchester (May 2017). These naturally result in significant coverage of ISIS and the attack itself. However, the way such events are covered often provides pathways to a network of ISIS produced content, which someone seeking to locate that content could follow – even if they had no prior knowledge about the group. It is worth pausing to consider how easy the process can be.

One might imagine a 'naïve searcher' who has heard about an attack and is inspired, as a result, to find more ISIS content to learn about the group. They may start by reading articles in online versions of newspapers. These articles frequently discuss how ISIS had made suggestions about attacks in their magazines, including *Rumiyah*.[80] Our 'naïve searcher' might now use the term 'Rumiyah' to search for the magazine. On 24 May, a test search using google.co.uk for 'Rumiyah' delivered the four top results:

76 John Hagel and Arthur G. Armstrong, *Net Gain: Expanding Markets Through Virtual Communities*, (Harvard Business School Press: Boston,1997). Also see Peter Morville, *Ambient findability: What We Find Changes Who We Become*, (O'Reilly Media: Sebastopol, 2005).

77 'Mosul battle: Last bridge "disabled by air strike"', *BBC News*, 27 December 2016, http://www.bbc.com/news/world-middle-east-38442811; BBC Audience figures, http://www.bbc.co.uk/mediacentre/latestnews/2016/bbc-weekly-global-audience.

78 Daily Mail Online circulation figures, http://www.adweek.com/digital/daily-mail-now-posting-650-videos-day-and-getting-383-million-monthly-views-171439/.

79 'Warning, Extremely Graphic Video: ISIS burns hostage alive', Fox News, 3 February 2015, https://video.foxnews.com/v/4030583977001/warning-extremely-graphic-video-isis-burns-hostage-alive/#sp=show-clips. The video projects the full legitimacy in the viewpoint of ISIS why the burning to death of Mu'adh a-Kassasiba is a legal act sanctioned by religious sources in times of war within the greater framework of "an eye for an eye".

80 Lizzie Dearden, 'Manchester bombing: Isis claims responsibility for concert attack as part of "shock and awe" tactics, analysts say', *Independent*, 23 May 2017, http://www.independent.co.uk/news/uk/home-news/manchester-bombing-isis-responsibility-salman-abedi-ariana-grande-concert-shock-awe-tactics-syria-a7752056.html?cmpid=facebook-post.

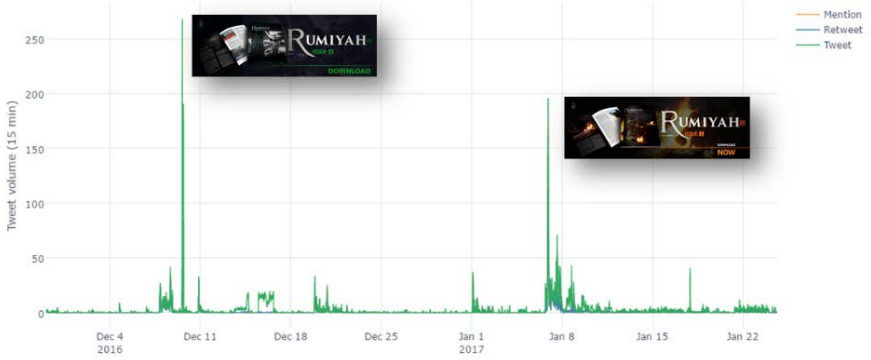
1) The Wikipedia page describing the magazine
2) An article about 'the latest Issue of Rumiyah' posted by the US based Clarion Project.
3) The link to the English language results for #Rumiyah on twitter
4) A PDF titled "Rome Magazine #8"

Of these results, only the Wikipedia page did not immediately provide access to the magazine. The second result led to the webpage of the Clarion Project, which provided access to all releases of *Rumiyah* (as well issues 1-15 of the ISIS magazine *Dabiq*).[81] A Twitter search of the same term delivered analogous results, which include a series of academics and commercial organisations sharing content from the magazine.

As this simple example shows, any hypothetical 'naïve searcher' would have access to multiple issues of an ISIS magazines with a single internet search, using only the name 'Rumiyah' found in an article in major UK newspaper. Social media is clearly a critical part of the issue, but as illustrated here, the actions of a wider penumbra of commentators and experts inadvertently help to ensure that ISIS media is easily findable.

Rumiyah Distribution: A Lesson in 'Findability'

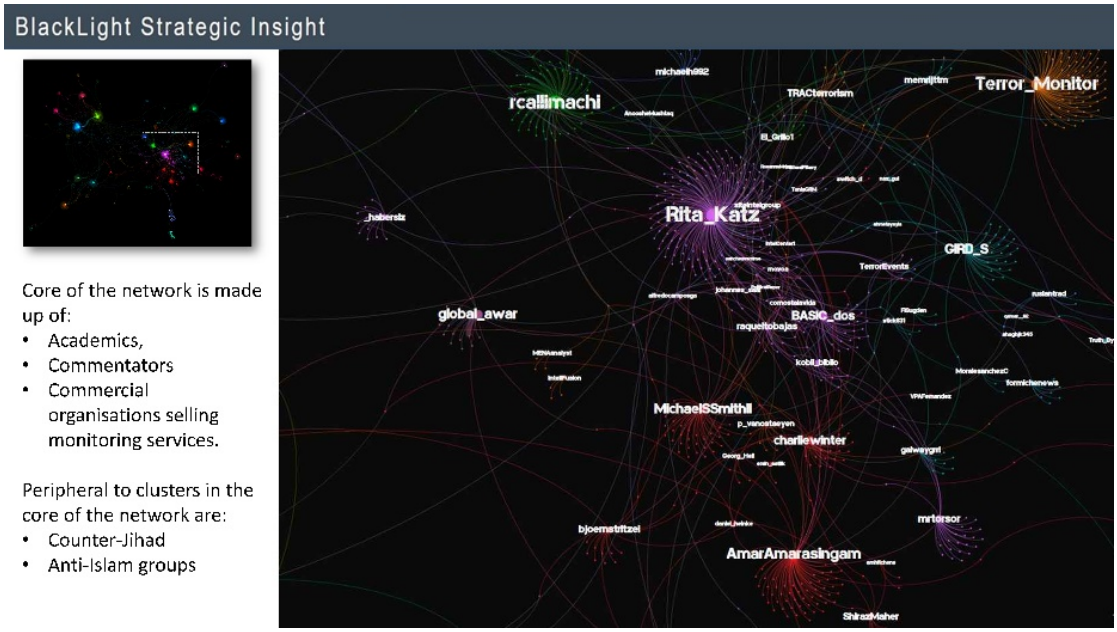
The root of the easy 'findability' of *Rumiyah* is the distribution network. During the initial release of an edition of the magazine, there is a surge of content about it on Twitter. This is shown in the graph below.



Closer analysis of the data reveals that there are relatively few original tweets, but many retweets. This indicates that there is little conversation and instead a greater focus on information distribution. Content within the spikes includes pictures of the front cover, links to download the magazine and related commentary. These spikes include accounts run by ISIS sympathisers who post links to the magazine, until their accounts are suspended.

81 The Clarion Project describes itself as challenging radical Islam and promoting Human Rights, http://clarionproject.org.

However, not all accounts that publish announcements of Rumiyah are suspended. Social network analysis (SNA) of the retweets, shows the structure of the network through which news of the magazine release flows. In the case of *Rumiyah*, SNA shows that information sharing about the magazine occurs via a series of loosely connected groups. This means the information is not dependent on a few individual Twitter accounts, which limits the effectiveness of account suspension. Equally, while Twitter suspends many ISIS accounts, the persistent presence for this content is provided for – in part – by non-ISIS organisations and commentators who also publish these announcements, as shown by the network graph below.



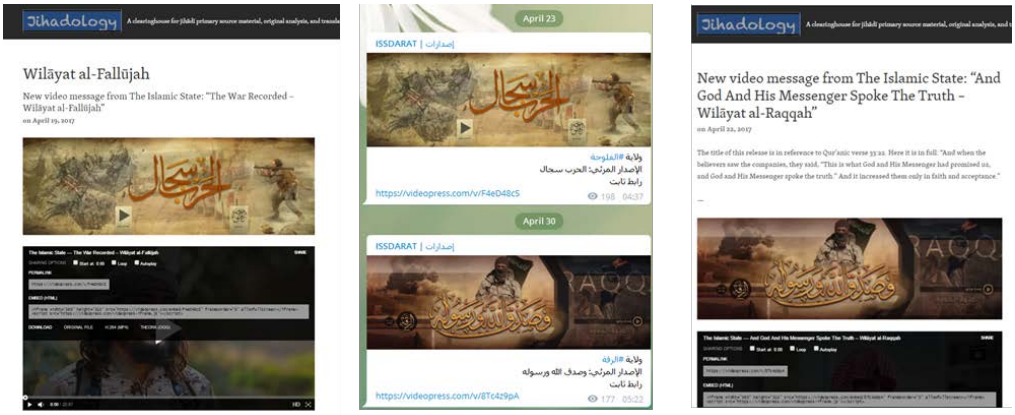
SNA demonstrates that, as news of a release spreads important nodes emerge as hubs for information dissemination. A critical number of these nodes are accounts run by non-ISIS organisations and individuals.

As a result, while CTIRU, EUROPOL and Twitter are making efforts to reduce the circulation of ISIS content on social media – the actions of some academics, mainstream media institutions and for-profit organisations appear to be inadvertently disseminating that content to a wide audience. A critical number of these nodes are accounts run by non-ISIS organisations and individuals, including some affiliated with universities in the UK.

Moreover, because these individuals and organisations use accounts, which are not suspended, the content enjoys greater longevity on Twitter than it otherwise would – making it more easily 'findable' to those searching for it. This factor is often overlooked in discussions of ISIS use of social media, which leads to an underappreciation of the reach and longevity of ISIS content on Twitter.

Unfortunately, ISIS supporters have realised that content posted by academics is permitted to remain online and on social media, whereas 'ISIS' accounts sharing the same content are suspended. This means the media mujahidin, their supporters, and other members of the jihadist movement know where their content will remain online. After the initial release of a video, ISIS Telegram channels follow-up with a second batch of links once the initial removal efforts have died down. These links often direct the user to more respectable 'hosts' of ISIS content.

To give but one example of this dynamic in action, one location that jihadist media operatives frequent to find ISIS content is Jihadology.net, run by the US-based academic, Aaron Zelin. Zelin's website has established itself as an important repository for researchers – and much of what it offers is provided in 'safe' format. Nonetheless, it is clear that his otherwise valuable work is being exploited by those who see in it an opportunity to circumvent the process of content removal. As the following screenshots demonstrate, ISIS followers have linked directly to material available on his site:



Left and middle top: Video from Fallujah posted on Jihadology using videopress 19th April, identical link posted by ISIS Telegram Channel 'Issdarat' on 23rd April.

Right and middle below: Video from Raqqa posted on Jihadology using videopress 22nd April, identical link posted by ISIS Telegram Channel 'Issdarat' on 30th April.

The normalisation of ISIS content sharing becomes even more problematic when it spills over into the news media. Following the Westminster attack, as is common after attacks that appear to be ISIS inspired or directed, images were produced by jihadist supporters in order to capitalise on the event. With attention focused on London, news organisations went in search of content. Unfortunately, some were then inclined to reproduce it in unvarnished form.

Announcing and publishing ISIS content is a regular feature of some contemporary journalism. Commentators often post the titles and images of jihadist publications, and even #tags, so any curious user looking for Islamic State content can refine their search for the authentic content. This type of exposure, reaching millions of viewers and readers, significantly expands the reach of Islamic State content and ensures it is more findable and persistently available than it otherwise would be.

As mentioned, one unhappy consequence of all this is to seriously complicate the efforts being made by CTIRU, EUROPOL and others, to reduce the spread of extremist content. It equally massively complicates the task social media companies face in rapidly detecting and removing ISIS content and suspending accounts, as a cull of all accounts sharing these images would impact on major news organisations, journalists and academics all of which would likely strongly protest having their accounts suspended.

Of course, researchers conducting genuine research undoubtedly need to be able to share material, but there are plenty of ways to do that without directly benefitting ISIS. Journalists and academics need to communicate, but that can happen without reposting raw, unadorned original content via social media. It is crucial, therefore, that those seeking to analyse and commentate upon the global jihadist movement are conscious of their own responsibilities when it comes to online behaviour.

Needless to say, even if such academics stopped publishing ISIS content on social media, and news organisations decided to no longer make videos available, the speed, agility and resilience of the media mujahidin would still present a significant challenge. However, **it is imperative that each organisation and individual takes responsibility for their own behaviour to ensure they do not amplify the reach and findability of content, however inadvertent that may have been in the past.**

At present, the jihadists appear to be at least one step ahead of those seeking to stop them. In this respect too, it is possible to be critical of the approach taken by some commentators and analysts, who have perhaps been too quick to embrace a narrative centred on the decline of ISIS' online presence.

The Myth of Decline?

Over the last year, much has been made of the relative decline in pro-ISIS tweets and content, largely based on studies which placed a high degree of emphasis on Twitter.[82] As Michael Lumpkin, head of the Global Engagement Center, has stated: 'We're denying ISIL the ability to operate uncontested online, and we're seeing their social media presence decline'.[83] As part of its information war against ISIS, the US Government made figures available that showed Twitter traffic for ISIS has gone down 45%.[84]

However, while such references to declining media production are frequent, in November 2016 Amaq released more than 30 videos from Mosul alone, in addition to numerous Amaq videos from other locations and videos produced by media foundations and *wilayat* (provinces). With this high volume of content being shared, and inspiring attacks – including the assassination of the Russian Ambassador[85] – why do highly publicised studies indicate a 'significant decline' of ISIS online output and media strategy?

In one sense the answer is simple: while many studies still focus solely, or almost exclusively on Twitter as the locus of ISIS 'core content', they fail to appreciate that the group has made a strategic shift to build a significant presence on Telegram. Too many studies thus miss the functional specialisation that has occurred in ISIS' online efforts. As described, Telegram is now the principal vehicle by which core content is communicated to active ISIS supporters; this content is then disseminated outwards across a wider information ecosystem, through which content is distributed to sympathisers. This is extremely effective. And one additional result is that a portion of the communication which would previously have occurred on Twitter now occurs on Telegram, out of the view of some researchers.[86] **The simple truth is that just because researchers cannot find it on Twitter does not mean the jihadist movement is in decline.**

Furthermore, too often researchers rely on a linear interpretation of 'success', such as counting pieces of content, or the number of ISIS followers, which appear to show a reduction in pro-ISIS content.[87] For example, a RAND study using Lexical analysis[88], claimed to detect 'a clear decline in the number of Islamic State supporters tweeting on a daily basis' starting in April 2015. The report's authors suggested two potential causes; 'first, the reduction may be a result of the Twitter suspension campaign', and second, 'the trend may partly be an indication of reduced global support for Islamic State'.[89] Similarly, analysis published by the Combating Terrorism Center (CTC), pointed to an alleged decline in the monthly number of 'videos, picture reports, and photographs embedded in Twitter posts' measured from January 2015 to August 2016. This report concluded: 'it is clear that the organization has been forced to cut back these [media] activities in response to the increasing amount of counterterrorism pressure brought to bear against the organization'.[90]

Yet neither the RAND nor CTC studies account for shifts in ISIS communication strategy and tactics, nor the agility of the media

82 It is unclear that a decline in the volume of content would indicate a decline in the organisation. For example, if an organisation released a four-part video as four 15 minute sections rather than as a single one hour video it would mean it was being more or less successful.

83 Bradley Klapper, 'Islamic State's Twitter traffic drops amid US efforts', *Associated Press*, 9 July 2016, https://apnews.com/21c9eb68e6294bdfa0a099a0632b8056/ap-exclusive-islamic-states-twitter-traffic-plunges.

84 Ibid.

85 Although no group has claimed responsibility for the attack, Islamic State media groups were fast to capitalize the assassination by providing the theological framework for such types of assaults. On 21 December 2016, a document was disseminated on Telegram authored by Abu Mu'adh al-Shammari, "limadha hakamna 'ala qatil al-safir bi-l kufr?", Ashhad Media. The title translates to "why have we ruled the killer of the ambassador [being a] disbeliever", cautioning that the intentions of the assailant are unknown to Islamic State and underpinning the fact that he had been serving the Turkish security forces. What matters for Sunni extremists, is a clear stated "pure intention". The author warns, "there is no proof given to us that the assassin reverted [to true Sunni Islam as defined by Islamic State], repented and declared his dissociation from this polytheistic group", referring to Islam as defined by Erdogan. While the killing of the ambassador is praised, the true intentions of his killer are questioned by Islamic State.

86 ISIS used to conduct communication with core supporters and da'wa on Twitter. By moving core communications to Telegram, this would naturally cause a drop in Twitter traffic. However, this indicates the core communication is going on elsewhere due to the change in platform not a decline in the group.

87 For example: J.M. Berger, *Twitter*, 20 September 2014, https://twitter.com/intelwire/status/513303666368196608; J. M. Berger and Jonathon Morgan, 'The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter', The Brookings Project on US Relations with the Islamic World, Analysis Paper No. 20, March 2015, https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf; J.M. Berger and Heather Perez, 'The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters', George Washington University Program on Extremism Occasional Paper, February 2016, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf.

88 Lexical Analysis is used to identify key themes and content for large text based data sets. It works by comparing the proportional frequencies of words in a target corpus against the proportional frequencies of the same words in a baseline corpus. See Appendix B in Elizabeth Bodine-Baron, Todd Helmus, Madeline Magnuson and Zev Winkelman, 'Examining ISIS Support and Opposition Networks on Twitter', RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1328.html.

mujahidin. The RAND study focuses on a variety of terms for ISIS. However, during the time period of the study, ISIS supporters increasingly used tags relating to a specific province, which are not included in the list of search terms used in the study.[91] An apparent lack of access to the nuances of jihadist strategy, meant that, however good the lexical analysis, data collection was not looking in the right place. Similarly, the CTC study focused on visual content disseminated predominantly via Twitter yet, during the relevant period of data collection, ISIS shifted away from pushing new content to their vanguard via Twitter, preferring instead to rely on Telegram.[92] While the CTC report noted that 'media products' were 'distributed on Telegram first', before being 'posted to public and open venues such as Twitter and websites', the study specifically excluded analysis of content posted on the former content.[93]

Moreover, what approaches of this kind fail to account for, is the extent to which social media platforms are fundamentally social networks. The metrics about followers that Twitter produces are accurate for an individual account, but cannot simply be aggregated to show either the total, or average number of followers in a specific network. If number of followers is aggregated, it will likely produce wildly inflated numbers for reach, and equally overstate any decline in ISIS social media.

The "falling follower fallacy" is demonstrated in the image below. In it, the same nodes are shown connected in different configurations, similar to the three types or topologies John Arquilla and David Ronfeldt highlighted in their discussion of 'Netwar'.[94] It demonstrates that average follower numbers can fluctuate widely, while the real number of users in the network remains the same.

89 Ibid.

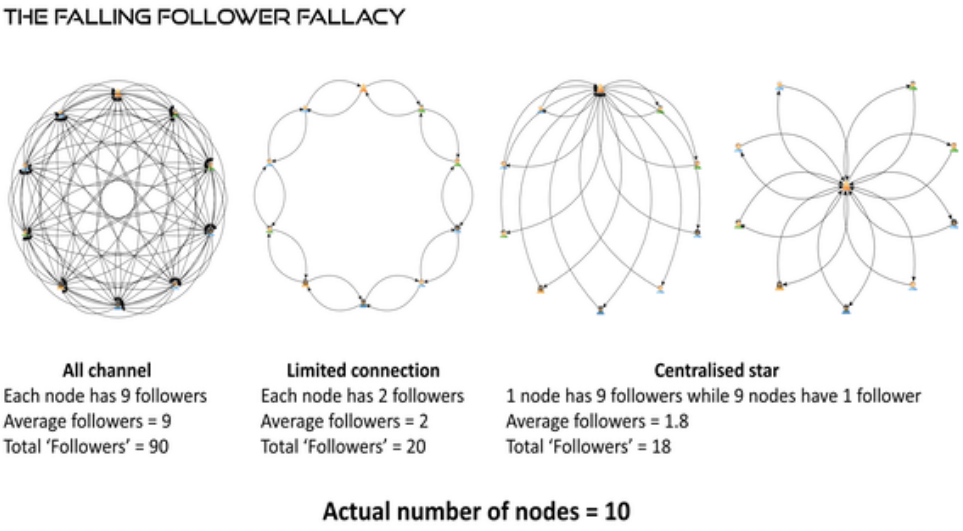
90 Daniel Milton, 'Communication Breakdown: Unravelling the Islamic State's Media Efforts', Combating Terrorism Center at West Point, October 2016.

91 Some tweets will have used both terms for the state and the province, but many do not.

92 Siyasa al-nashr fi mu'assassat al-wafa' li-l intaj al-i'lami, al-Wafa' Media, 13 December 2016.

93 Daniel Milton, 'Communication Breakdown: Unravelling the Islamic State's Media Efforts', Combating Terrorism Center at West Point, October 2016.

94 John Arquilla and David Ronfeldt, The Advent of Netwar, RAND Corporation, 1996, https://www.rand.org/pubs/monograph_reports/MR789.html.



Reading left to right, the different layouts above demonstrate that:

- Aggregating follower numbers inflates the number of accounts that appear to be in the network.
- The decline in aggregated follower numbers cannot be read as showing decline in the number of accounts in the network.
- The decline in aggregated follower numbers cannot be used to show that the network is being disrupted.

ISIS strategy was, and still is, to distribute content, not get followers on social media. Thus, proxy metrics such as average follower numbers are not a substitute for an accurate assessment of what it is that ISIS seeks to achieve.[95]

In the wake of the June 2017 attack in London, commentary using these proxy metrics resurfaced again, claiming the position of ISIS on 'open platforms like Twitter and Facebook has remained under heavy pressure'. This data led to the conclusion that 'efforts to control IS on open social media platforms' had reached 'the point of diminishing returns', with 'not much room left for large-scale improvements'.[96] The underlying assumption again seemed to be that the fight, on Twitter at least, had been largely won. This echoed the claims of the UK Home Office-funded research project produced by VOX-Pol that stated, 'the IS Twitter community is now almost non-existent'.[97] Yet as our research demonstrates, this is surely too optimistic a verdict, given that Twitter remains the top referrer to some ISIS content.

The enduring obsession with counting pieces of content, without reference to the strategic purpose underlying it, provides little basis for the attendant conclusions. Contrast, for example, the release of an hour-long video with the release of four fifteen minute videos: does the release of four short videos make ISIS more successful than one long video? Do two pictures represent twice the success of one picture? How about 'GIFs' and 'stickers' on Telegram – what is their comparative value to a photo?

95 Ironically, this second wave of 'Islamic State in decline' reports put the high point of Islamic State content dissemination well after the first wave of claims had been made.

96 J.M. Berger, '"Defeating IS Ideology" Sounds Good, But What Does It Really Mean?', ICCT, 6 June 2017, https://icct.nl/publication/defeating-is-ideology-sounds-good-but-what-does-it-really-mean/.

97 Conway et al., 'Disrupting Daesh', p. 45.

Perhaps more problematic with the 'counting' approach is the meaning attached to fluctuations in content. As we have tried to show, a decline in tweets or content on Twitter does not necessarily equate to a substantial decline in the *accessibility* or *reach* of content being distributed. Nor is it an indication of decline in the physical presence or potential of the jihadist movement. Notice how little content ISIS produced before its forces swept across large parts of Iraq and Syria. If content production were an indicator of military potential or success achieved – one would expect production at that time to be near its height - yet it was not. If studies consider only the period since the declaration of the Caliphate, they miss the nuance in the content and the long-term fluctuations of the jihadist movement.

A recent comparison of content produced in the summer 2015 and February 2017, suggestively entitled 'The ISIS Propaganda Decline', claims to identify 'a productivity drop of approximately 36 percent'.[98] There are a number of major difficulties with this conclusion. First, it is the comparison of a random month (Jumada al-Awwal – largely equivalent to February 2017) with the summer of 2015. Summer 2015 featured the first Ramadan in the Caliphate, the first anniversary of the Caliphate, and coincided with the launch of the wilayat as the dominant source of ISIS content. One may be unsurprised to learn that this resulted in a large quantity of content being produced in summer 2015 – just as there was, to draw a frivolous analogy, a vast amount of coverage, and a huge number of images of the Queen during her Diamond Jubilee celebrations – far in excess of a 'normal' month. Summer 2015 was in fact an aberration, in comparison to the period up to and including spring 2015 and subsequently autumn/winter of the same year. This is shown in the longitudinal video production data gathered between 2013 and 2017 (as discussed above, see pages 31-33).

Another problem here is that the impression of decline was created by drawing a line between only two discreet points in time. Two points are very rarely a useful way to identify a trend. For example, using the same approach one finds there was a 617% increase in images produced, when the last week in August 2016 is compared with penultimate week in April 2017; a comparison of the second week in October 2016, to April 2017, shows a 509% increase. But neither of these are a genuine cause to conclude that ISIS is experiencing a surge in output – any more than the comparison of two other points would provide reason to talk of a decline.

In reality, by using a longitudinal approach and a rolling mean to compare weekly production across 2016 and 2017 (see above, pages 32-33), we can demonstrate that Jumada al-Awwal (February 2017) was a period of *increasing* production, after a dip towards the end of 2016. In addition, data from shortlinks (see above, page 42) highlights the fact that ISIS has been able to drive considerable traffic towards the content it created in the spring of 2017. Perhaps most pertinent is the fact, as previously noted, that 40% of traffic for which a referring domain is known, came from Twitter, with a further 12% coming from Facebook (see pages 42-43).

98 Charlie Winter, 'The ISIS Propaganda Decline', ICSR Insight, 23 March 2017.

To conclude, this chapter has tried to show why much recent research has erred in identifying a decline in ISIS' social media activity. **The reality is that the online jihadist movement has been able to:**

- **continue producing content at a broadly consistent rate over the long-term;**
- **distribute content via numerous social media and digital platforms including Facebook and Twitter; and**
- **reach users around the globe and in the UK specifically.**

The truth of all this means that we surely need to revisit our approaches for dealing with this threat. At present, putative solutions are not delivering success; and for this reason, it is worth considering what options for change are available.

Part Two: What is to be done? Options for Future Policy

Future policy to counter the jihadist movement must account for the breadth of the challenge at the strategic level. Hitherto, governments and the security services have been drawn into a rather fruitless process of 'whack-a-mole', in which precious energy and resources are wasted on the removal of individual pieces of content. We need to go beyond this to disrupt the jihadist dissemination network and severely curtail its impact.

Of course, our response needs to retain a sense of balance and proportionality. We should also be cognisant of the fact that jihadists want to securitise western society – to undermine the liberal values at its core. They also want to eliminate the 'grayzone', which is to say the social and cultural space that, in their view, allows Muslims to live freely and prosperously within western societies. Their goal instead is to force the world into two distinct camps: that of the Islamic '*umma*' lined up behind the Islamic State, on the one hand; and on the other, that of unbelief – namely 'the West'.[99] For this reason, we should be ever mindful of playing into their hands.

And yet, it is clear that we cannot stand idle. Earlier this year, the Prime Minister rightly said that 'enough is enough' and that change was required – given the gravity of the terrorist threat. She spoke of the need for 'difficult conversations' – and it is in that spirit that this section explores possible options for future policy. The aim here is not to provide a rigid template for things that must be done; rather, the hope is to initiate a debate around a number of different issues – to challenge conventional wisdom and ask, in a spirit of genuine inquiry, what can be done about the problem of online extremism.

A core premise for what follows is the belief that the scale of the threat requires a comprehensive, 'all of society' approach. The aim must be to reduce the availability of, and public exposure to, jihadist content online – to dry up the extremist supply line in every way possible. A key theme is that of responsibility: different sectors in society must be encouraged to shoulder their responsibilities in such a way that they reduce, rather than exacerbate the problem.

99 Dabiq, Issue 7.

Ethical Conduct by Researchers

As described in part one, it is clear that academics, journalists and commentators are inadvertently aiding in the dissemination and durability of much jihadist content online. They are making the job of the security services and internet companies harder, whilst extending the reach of groups like ISIS. Here the approach taken by those studying the use of the internet to share indecent images of children could be a useful example. They conduct academic research while posting neither the images nor running commentary on social media.[100]

Just as many have called for social media companies to be responsible for the use (and abuse) of their platforms, media outlets, journalists and researchers must be far more careful when it comes to (re-) posting content that, however inadvertently, amplifies the reach of ISIS. As this research has shown, it is not academic research per se, that is the problem, but the careless dissemination of ISIS content and announcements on social media and public blogs, which increases its findability and availability.

A simple and easy first step would be to encourage researchers/journalists to sign up to an ethical code of conduct, specifically focused on those who study illegal groups and content. Many universities already have research guidelines and some areas of research have ethics committees to approve research projects. As such, the ethical review of academic research is already an accepted norm in many fields. If sharing content from illegal groups via social media is considered part of research, the norm of ethical review should apply. If it is not part of research, claims of consideration for 'academic freedom' to share illegal material may not hold much water, particularly as many twitter accounts are used in a 'personal' rather than 'professional' capacity.

This approach, which could be developed by universities in the first instance, would not impinge on searching for, nor possession of, content for research purposes. Nor would this approach inhibit the publication of vital academic research into the nature of a group deemed illegal in the UK. **It would however, be a small step in limiting the spread and findability of content, reduce the normalisation of sharing content from illegal groups, while also allowing CTIRU, EUROPOL and social media companies to focus their resources on the spread of content from real pro-ISIS accounts**.

The Home Affairs Select Committee might in future ask universities or media outlets what they have done to ensure the research of illegal content is done in a safe, ethical way, which does not render the raw content easily accessible for public consumption via blogs and social media. As this has been achieved in areas such as child protection and the study of indecent images of children, it should be possible to do similar with magazines that contain a justification of the burning alive of captured soldiers.

A new, ethical code of conduct for this field might include pledges:

100 For example: Ethel Quayle and Terry Jones, 'Sexualized Images of Children on the Internet', Sexual Abuse: A Journal of Research and Treatment, Vol. 23, Issue 1, 2011, pp. 7-21.

- not to re-post original jihadist content in raw, unadulterated form, except where it is part of a research publication, or placed alongside critical analysis;
- not to re-post, in real time, the hashtags that drive the dissemination of jihadist content on social media;[101]
- not to re-post visual logs, or images of Telegram channels, live accounts and account names, which allow those less well informed to find those channels; and
- if seeking to provide a library/repository of jihadist materials, to implement a subscription list/log-in requirement that would de-incentivise those seeking to exploit such services to actively promote jihad.

To be clear, the goal here is certainly not to impede journalistic and academic research endeavours – these have an important role to play in understanding the meaning and character of the broad jihadist movement. Instead, the aim is simply to make sure that those wishing to be part of the solution, are not making the problem worse.

Drying up the Online Supply: The Internet Companies

Over the last several years there has been a groundswell of opinion demanding that the leading social media companies do more to tackle the scourge of online extremism. In 2014, Robert Hannigan, then the incoming Director of GCHQ focused attention on those companies, which he labelled, 'the command-and-control networks of choice' for jihadist extremists; he called for them to cooperate more closely with the government and to make greater strides to remove extremist material.[102]

Elsewhere, the Home Affairs Select Committee has emerged as a relentless critic of the social media companies. In August 2016, the Committee said that Facebook, Twitter and YouTube (owned by Google) were the 'vehicle of choice in spreading [extremist] propaganda' and acted as 'recruiting platforms for terrorism'; they were said to be 'consciously failing to combat the use of their sites to promote terrorism and killings'.[103] In a further report examining anti-Semitism in the UK, the Committee described it as 'deplorable' that Twitter should act as an 'inert host for swathes of anti-Semitic hate speech and abuse'. There were calls for the 'proactive identification' and removal of abusive users.[104]

More recently still, the Committee has accused the mainstream social media companies of 'commercial prostitution' for failing to police their content.[105] Google was accused of 'profiting from hatred' – because of adverts placed on sites carrying extremist content. This led numerous companies, including Marks & Spencer, McDonald's and L'Oreal to withdraw their adverts.[106] The Home Affairs Select Committee charged the 'biggest and richest social media companies', with being 'shamefully far from taking sufficient action to tackle illegal and

101 Attempts at 'flooding' hashtags with anti-ISIS content have regularly failed to disrupt distribution of content and instead raise the profile of the tags amongst social media users.

102 Robert Hannigan, 'The web is a terrorist's command-and-control network of choice', *The Financial Times*, 3 November 2014, https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0.

103 House of Commons, Home Affairs Select Committee, *Radicalisation: the counter-narrative and identifying the tipping point: Eighth report of session, 2016-2017* (25 August 2016), § 38.

104 House of Commons, Home Affairs Select Committee, *Antisemitism in the UK: Tenth report of session, 2016-17*, (13 October 2016), §8-10.

105 Patrick Sawer, 'Social media firms accused of "commercial prostitution"', *Daily Telegraph*, 17 March 2017, http://www.telegraph.co.uk/news/2017/03/14/social-media-firms-accused-commercial-prostitution/.

106 Patrick Sawer, 'Social media firms accused of "commercial prostitution"', *Daily Telegraph*, 17 March 2017. The most recent HASC report states, 'The biggest and richest social media companies are shamefully far from taking sufficient action to tackle illegal and dangerous content, to implement proper community standards or to keep their users safe'. House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, (25 April 2017), p. 21, https://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf.

dangerous content'. It insisted that the companies 'be held accountable for removing extremist and terrorist propaganda hosted on their networks'.[107]

Beyond parliament, a succession of newspaper investigations highlighted the widespread availability of extremist content via mainstream social media platforms – often promoted by company algorithms.[108] Facebook's moderator guidelines, as leaked to the *Guardian*, showed that content, which most would consider deeply unpalatable did not fall foul of the rules.[109] And even pro-terrorist material flagged to moderators, such as that which praised the Westminster Bridge attack in London, was not removed – on account of the fact that it did not breach 'community standards'.[110] In the run-up to the general election, it was reported that campaign adverts for the three main British political parties were appearing on YouTube next to videos of Islamic extremists, such as Sheikh Khaled al-Rashed – and that the channel in question was only suspended after *The Times* had drawn it to Google's attention.[111]

In the wake of the Westminster attack, Home Secretary Amber Rudd and Foreign Secretary Boris Johnson both criticised the internet companies over their failure to stop extremist content – and accused them of acting as a 'conduit' for murderous terrorists. Johnson called Google 'disgusting' for making money out of violent material and called on the internet companies to show more 'social responsibility'; he also urged the creation of new systems to detect and remove extremist content – and accused the companies of failing to act, even when given warnings about the material. Rudd meanwhile raised the possibility of changing the law – albeit whilst expressing a preference for an independent, industry-led approach.[112]

Perhaps most pointed, were the comments of the Prime Minister after the London Bridge attacks of June 2017. Theresa May called for decisive action to prevent the internet being used as a 'safe space' for extremism and radicalisation.[113] At the subsequent G7 summit she urged world leaders to do more to tackle online extremism and said that tech companies should raise their game, to identify and remove extremist content. The Prime Minister insisted that the industry had a 'social responsibility' to do more to remove harmful content.[114] And the result was a communique, which called for communication service providers and social media companies to 'substantially increase their effort to address terrorist content'. Industry was encouraged to pool resources to this end, with a view to developing new technology for the removal of extremist material.[115]

Soon after, the British and French governments produced their own 'action plan', aimed at preventing the internet being used as a 'safe space for terrorists and criminals'. This set four priorities: to improve methods for removing 'illegal content from the internet'; to 'support the efforts of civil society organisations to promote alternative and counter-narratives'; to cooperate on ensuring the security services could 'access data for investigative purposes'; and to 'improve access to digital evidence across borders'. For present purposes, the first of these was the most significant, as the French and British governments urged

107 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, HC609 (25 April 2017), §2-8.

108 Alexi Mostrous, 'Facebook publishing child pornography', *The Times*, 13 April 2017, https://www.thetimes.co.uk/article/facebook-publishing-child-pornography-pdgt87nm6; Alexi Mostrous, 'In-depth on terrorism: View Isis videos and befriend hundreds of jihadists on Facebook within days', *The Times*, 13 April 2017, https://www.thetimes.co.uk/article/view-isis-videos-and-befriend-hundreds-of-jihadists-within-days-htjnh3ws2.

109 Nick Hopkins, 'Revealed: Facebook's internal rulebook on sex, terrorism and violence', *Guardian*, 21 May 2017, https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence.

110 Alexi Mostrous, 'Facebook publishing child pornography', *The Times*, 13 April 2017; Alexi Mostrous, 'In-depth on terrorism: View Isis videos and befriend hundreds of jihadists on Facebook within days', *The Times*, 13 April 2017.

111 Alexi Mostrous, 'Election videos on YouTube hate channels', *The Times*, 7 June 2017, https://www.thetimes.co.uk/article/election-videos-on-youtube-hate-channels-d8pkb2k53.

112 James Tapsfield, 'Ministers slam internet giants such as Google and Facebook for "disgusting" failure to block extremist content accusing them of being "conduit" for murderous terrorists', *Daily Mail*, 26 March 2017, http://www.dailymail.co.uk/news/article-4350196/Ministers-slam-net-firms-failure-block-extremists.html; Tim Shipman, Simon Duke and Duncan Geddes, 'Boris savages "disgusting" Google', *The Sunday Times*, 26 March 2017, https://www.thetimes.co.uk/article/boris-savages-disgusting-google-7kc5tbzb6.

113 Alexi Mostrous, 'Isis unleashes internet propaganda to spur on others', *The Times*, 6 June 2017, https://www.thetimes.co.uk/article/isis-unleashes-sadistic-internet-propaganda-to-spur-on-others-bhf0fjv75.

114 Anushka Asthana, 'Theresa May calls on tech firms to lead fight against online extremism', *Guardian*, 26 May 2017, https://www.theguardian.com/politics/2017/may/25/theresa-may-calls-on-tech-giants-to-lead-fight-against-online-extremism.

115 Francis Elliott, 'World leaders back online crackdown', *The Times*, 27 May 2017, https://www.thetimes.co.uk/article/world-leaders-back-crackdown-on-online-extremism-0ml5z70k2.

the internet companies to be more pro-active in their approach – identifying content automatically to prevent publication, rather than relying on users to flag content for deletion. In line with the Home Secretary's earlier appeal, the action plan called for the creation of an 'industry led forum', to 'develop technical and policy solutions to rapidly remove terrorist content on the internet', working alongside the existing EIRU and EUIF. The governments also held out the prospect of fresh regulation – to help clarify the question of what constituted 'unacceptable content online'.[116]

The 'Five Eyes' intelligence alliance has endorsed these efforts, producing a joint letter, which said it was 'critical' that more be done to remove extremist material and terrorist manuals from the internet. The correspondence reiterated the Prime Minister's line that there should be no 'safe space' for the transmission of extremist and terrorist material online.[117]

This cacophony of criticism has been echoed across the Atlantic, where the authorities have also considered changes to the legal framework. In the face of all this, the tech companies have slowly shifted ground. Where once they used to defer to arguments about the protection of free speech, or claimed to lack the power and/or expertise to intervene effectively against extremism, there have been signs of a greater willingness to act.[118] In response to criticism from the Home Affairs Select Committee, for instance, Google did remove some material from YouTube – including videos by the far right group, National Action. Though far from comprehensive – and white supremacist material remained available via the same platform – this was a sign that the collaboration between governments and companies could deliver progress.[119]

Google has also announced an action plan for increased safeguards and a broadening of the definition of inappropriate content, beyond the purely violent, to include 'incendiary and derogatory language' aimed at individuals on basis of religion or gender.[120] The company decided that adverts would no longer be placed on YouTube channels with fewer than 10,000 views – an attempt to prevent small, extremism-purveying 'rogue traders' from benefitting financially from advertising revenue.[121]

Yet, Google's initial proposals did not include plans to pro-actively filter out more extremist material. Instead, they continued to prefer a system that relied on user 'flagging' to identify hateful content.[122] And the response of businesses was described as 'lukewarm', with leading brands wanting to see actions over words.[123] In the same vein, Facebook's headline-grabbing announcement that they were employing an extra 3,000 people to moderate content (in addition to some 4,500 people already reviewing posts), was described as providing 'false reassurance' by one cybercrime expert, who also noted that 'human moderation', as an approach, was utterly impractical.[124]

More encouraging was the announcement that Facebook had developed artificial intelligence, which used algorithms to identify postings and accounts linked to terrorism — with a view to suspending, or removing material.[125] In parallel, Google too has said it

116 'French-British action plan: internet security', Cabinet Office and Home Office, 13 June 2017, https://www.gov.uk/government/publications/french-british-action-plan-internet-security.

117 'Five Eye countries join Britain's call to remove terror content online', Home Office, 28 June 2017, https://www.gov.uk/government/news/five-eye-countries-join-britains-call-to-remove-terror-content-online; '"Five Eyes" nations back web terror fight', *Evening Standard*, 28 June 2017.

118 Celia Kang and Matt Apuzzo, 'U.S. Asks Tech and Entertainment Industries Help in Fighting Terrorism', *The New York Times*, 24 February 2016, https://www.nytimes.com/2016/02/25/technology/tech-and-media-firms-called-to-white-house-for-terrorism-meeting.html?mcubz=3.

119 Richard Ford, Fiona Hamilton and Deborah Haynes, 'Tommy Robinson accused of exploiting Finsbury Park assault as far-right fans flames of hate', *The Times*, 20 June 2017, https://www.thetimes.co.uk/article/tommy-robinson-accused-of-exploiting-finsbury-park-assault-as-far-right-fans-flames-of-hate-50p8dssd3.

120 Madhumita Murgia, 'Google unveils advertising safeguards as backlash over extremist videos rises', *The Financial Times*, 22 March 2017, https://www.ft.com/content/46475974-0e30-11e7-b030-768954394623.

121 Samantha Masunaga, 'YouTube won't put ads on channels with fewer than 10,000 views', *The Los Angeles Times*, 7 April 2017, http://www.latimes.com/business/la-fi-tn-youtube-ads-20170407-story.html.

122 Simon Duke, 'Google pressed to cut prices as extremist ads fury mounts', *The Sunday Times*, 26 March 2017, https://www.thetimes.co.uk/article/google-pressed-to-cut-prices-as-extremist-ads-fury-mounts-nrgffwq73.

123 Matthew Garrahan, 'Advertisers skeptical on Google ad policy changes', *The Financial Times*, 22 March 2017, https://www.ft.com/content/dea0e14e-0e59-11e7-a88c-50ba212dce4d.

124 David Sanderson, 'Facebook use of young moderators "unethical"', *The Times*, 1 June 2017, https://www.thetimes.co.uk/article/facebook-use-of-young-moderators-unethical-kwp6xhgts.

125 Sam Schechner, 'Facebook Boosts A.I. to Block Terrorist Propaganda', *The Wall Street Journal*, 15 June 2017, https://www.wsj.com/articles/facebook-boosts-a-i-to-block-terrorist-propaganda-1497546000.

will allocate more resources to developing artificial intelligence to identify and remove extremist content. Further, the company stated that it would work more closely with charities and counter-extremism groups, who could act as 'trusted flaggers' of problematic material – including that which did not explicitly violate its community guidelines (though such content, it should be noted, was not to be removed – merely prefaced with a warning and denied any revenue or space for endorsement).[126] Most recently, Google announced that YouTube would automatically redirect searches for ISIS material towards counter-messaging videos that challenged, or sought to debunk, aspects of the jihadist narrative.[127] Taken together these latest initiatives represent progress. Along with the more active use of spam filters by Twitter, they may well help to reduce the availability of content.

The leading lights within the social media industry do at least now seem more cognisant of their responsibilities. In December 2016, it was announced that the principal companies – Facebook, Google, Twitter and Microsoft – were planning to coordinate efforts to combat extremist material online. Under this initiative, they would work to create a shared 'database of unique digital fingerprints' (or 'hashes'), which would allow for the rapid identification and removal of extremist content. The assumption was that the project would draw on the National Center for Missing and Exploited Children's PhotoDNA technology, which Microsoft had developed for tackling images of child sexual abuse.[128]

On the face of it, such an initiative seemed extremely promising. Yet, the problem with the scheme is that it appears to follow a 'lowest common denominator' approach. As a result of the fact that the companies, like national governments, each define 'extremism' and protect 'free speech' in a different way, their cooperation can only proceed by targeting the most egregious forms of material on which everyone can agree. Given the afore-mentioned latitude in the way in which 'community standards' guidelines have been interpreted to-date, this can only be a part of the response – targeting some content automatically to release resources to focus on more controversial content.

Moreover, little has been done to actualise even this relatively limited approach. In late June 2017, the same four biggest companies (Facebook, Google, Twitter and Microsoft) – announced, with much fanfare, the establishment of a 'Global Internet Forum' to tackle terrorism.[129] Yet, it is salutary to note that it had taken six months to reach even this point – of agreeing to talk together about the issue – and this, against a backdrop of fairly concerned governmental pressure and public concern. For this reason, it is perhaps no surprise that many remain sceptical about how much 'will' exists in Silicon Valley to deal with this problem.

To many, the frustration is that the same companies have shown a capacity for more robust and obviously interventionist approaches when it comes to tackling, for example, the scourge of child pornography – though even here, gaps remain.[130] Similarly, they have

126 Mark Bridge and Francis Elliott, 'Google finally gets tough over hate videos', *The Times*, 19 June 2017, https://www.thetimes.co.uk/article/under-fire-google-finally-gets-tough-on-hate-videos-mk8c3lf8g.

127 'YouTube to redirect searches for IS videos', *BBC News*, 21 July 2017, http://www.bbc.co.uk/news/technology-40681625.

128 'Facebook, Twitter, Google and Microsoft team up to tackle extremist content', *Guardian*, 6 December 2016, https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content.

129 Sam Levin, 'Tech giants team up to fight extremism following cries that they allow terrorism', *Guardian*, 26 June 2017, https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism.

130 With regards to the latter, see Alexi Mostrous, 'Facebook publishing child pornography', *The Times*, 13 April 2017; Alexi Mostrous, 'In-depth on terrorism: View Isis videos and befriend hundreds of jihadists on Facebook within days', *The Times*, 13 April 2017.

acted firmly to combat online music piracy and the proliferation of 'spam', devising technologies to identify and filter out such content.[131] The Home Affairs Select Committee noted that Google could 'act quickly to remove videos from YouTube' when they were 'found to infringe copyright rules', but the 'same prompt action' was 'not taken when the material involve[d] hateful or illegal content.'

Elsewhere, it is striking that even as the pace of technological innovation for dealing with extremist content remains slow, one sees news of, for example, Facebook developing new facial recognition software that can observe a user's emotional state in real time.[132] What this demonstrates is that when it suits their interests to act, the tech companies seem more than capable of doing so. And again, it is salutary to note the simple fact that the last year *has* shown that the companies are susceptible to public and political pressure for change.

So what should be done?

In contemplating this issue, an immediate difficulty that one encounters is the fact that most of the large platforms are based on servers located in the United States. Policy responses there are constrained by the First Amendment. Nevertheless, even in the US, a bill introduced by Senators Richard Burr and Dianne Feinstein, the chairman and former vice-chair of the Senate Select Committee on Intelligence, would require the internet platforms to report terrorist activity on their networks to law enforcement. The Burr-Feinstein bill is indicative of the extent to which the broader intellectual climate is changing on the question of online extremism. As the afore-mentioned words of the Prime Minister and her colleagues make clear, there is an appetite for change. The government has declared its intention to make the UK 'the safest place in the world for young people to go online', and launched a new 'Internet Safety Strategy'. This laudable initiative is one that can be built upon to tackle the threat from extremism more broadly.[133]

Of course, this does not mean that the threat can be eradicated entirely. But there is surely scope to make the online environment much less hospitable for extremist content. In this context, it is worth challenging the popular canard that is invariably a mistake to drive a phenomenon 'underground', or in this case, into the cyber undergrowth of the 'dark web'. Why would this not be a laudable aim? To drive extremism of all kinds – but especially its jihadist variant – out of mainstream social media platforms is surely a worthwhile objective. Why would one not want to stigmatise those hosting such material? After all, as has been described, a key strategic aim of ISIS and its fellow movements is to use this content for outreach and missionary work – to recruit new members and mobilise those sympathetic to their cause. That being so, the removal of their material from the mainstream would represent an important setback.

There is a broader debate here about the need for the mainstream companies to accept their corporate responsibilities. In line with this, they must accept their fundamental role as de facto distributors of

131 Dominic Kennedy, 'Social media giants fail to tackle hatred, say MPs', *The Times*, 1 May 2017, https://www.thetimes.co.uk/article/social-media-giants-fail-to-tackle-hatred-say-mps-kgw2k6mdv.

132 Mark Bridge, 'Facebook wants to analyse your emotions as you browse', *The Times*, 6 June 2017, https://www.thetimes.co.uk/article/facebook-wants-to-analyse-your-emotions-as-you-browse-8wrlb2hhb.

133 'Government launches major new drive on internet safety', Department for Digital, Culture, Media & Sport, 27 February 2017, https://www.gov.uk/government/news/government-launches-major-new-drive-on-internet-safety.

online content. Mark Zuckerberg's recent manifesto about the need for 'responsible capitalism' could serve as a useful point of departure for asking the tech companies what they are doing to ensure they behave 'responsibly' online. The Home Affairs Select Committee had it right when it stated, in its August 2016 report, that the leading tech companies, 'must accept that the hundreds of millions in revenues generated from billions of people using their products needs to be accompanied by a greater sense of responsibility and ownership for the impact that extremist material on their sites is having'. They were urged to adopt a 'zero tolerance approach to online extremism' and act as 'responsible operators'.[134]

The government should accept that it can usefully help to set the terms of trade on this issue; the authorities can help the mainstream tech companies to improve their game. In numerous other spheres, few would question this idea. When it comes to environmental protections, for instance, or the need to interdict the trade of 'conflict minerals', there appears to be far greater receptivity to the idea that government should intervene, or that companies must do more to prove that they are 'clean'.[135]

A critical aim of policy must be to shift the 'barometer of willingness' on the part of the companies to act. In recent months, there are signs that the needle has moved in a positive direction – the goal must be to continue that trend.

Of course, there are those who appear impervious to appeals for 'responsible behaviour'. Telegram wears its refusal to work with governments and security agencies as a badge of honour (though even Telegram has proclaimed its determination to remove channels that disseminate ISIS material – albeit with very limited success).[136] New, smaller platforms such as the far-right hosting Gab, appear even less inclined to police content.[137] And even the 'giants' of the industry at times seem less than resolute in their focus on the issue.

Despite this – indeed, perhaps because of it – there is surely merit in the government aiming to secure change. And it makes sense to start by focusing on the largest mainstream companies, precisely because of their own importance in helping to frame the actions and outlook of the social media industry as a whole.

In a stimulating recent article, Stuart MacDonald drew on the work of Ian Ayres and John Braithwaite to call attention to the notion of 'responsive regulation'.[138] This idea offers a useful paradigm for thinking about how government should deal with the social media companies – not least because of the 'compliance pyramid' outlined by Ayres and Braithwaite. This schema envisages a sliding scale of government policies vis-à-vis industry, which moves from attempts to persuade at the bottom, to more punitive measures at the top. The aim is to secure compliance with a given set of norms, or behaviours.

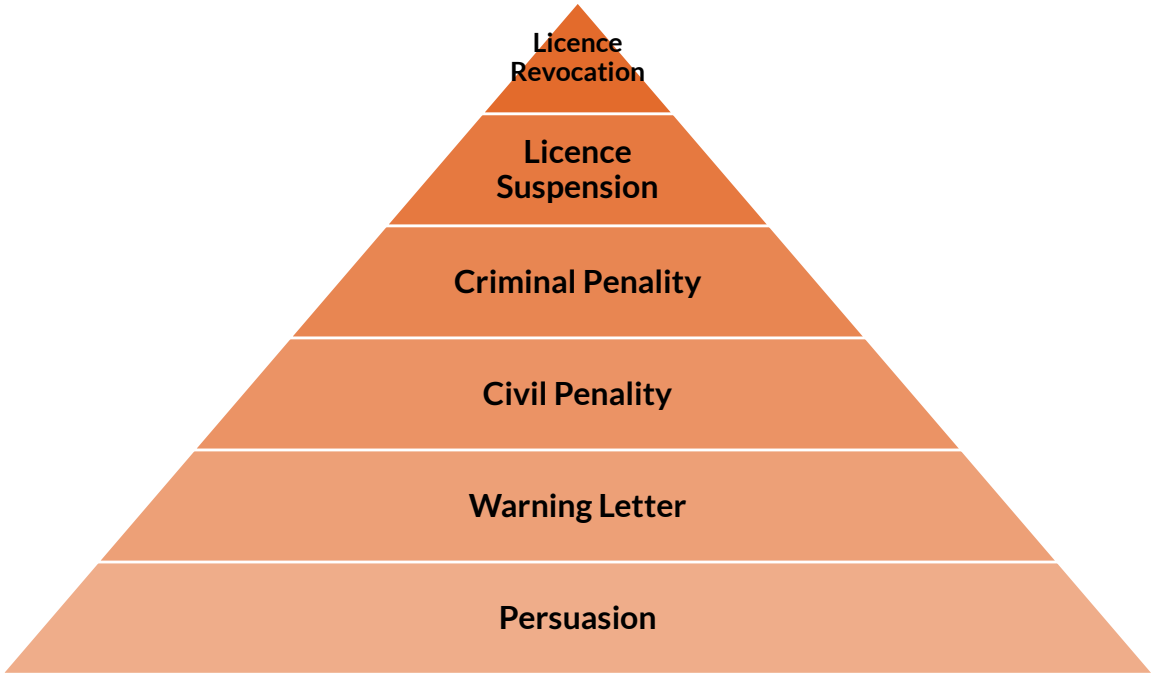
134 House of Commons, Home Affairs Select Committee, *Radicalisation: the counter-narrative and identifying the tipping point: Eighth report of session, 2016-2017* (25 August 2016), §38.

135 Kate Hodal, 'Tech companies must do more to avoid using minerals tainted by rights abuses', *Guardian*, 7 April 2017, https://www.theguardian.com/global-development/2017/apr/07/tech-companies-conflict-minerals-rights-abuses-verisk-maplecroft.

136 *Markus Ra, 'Don't Shoot the Messenger'*, Telegraph, 27 March 2017, http://telegra.ph/Don't-Shoot-the-Messenger.

137 Mark Bridge, 'Surge in support for Gab, a website that allows hate speech', *The Times*, 19 June 2017, https://www.thetimes.co.uk/article/surge-in-support-for-gab-website-that-allows-hate-speech-790mg09tw.

138 Stuart Macdonald, 'Radicalisers as Regulators: An Examination of Dabiq Magazine', *Terrorists' Use of the Internet: Assessment and Response*, NATO Science for Peace and Security Series - E: Human and Societal Dynamics, pp. 146-157, June 2017.



Source: Ayres and Braithwaite (1992)

In a context of 'responsive regulation', it is assumed that the preference of both the regulators and the regulated alike, is for a system of voluntary, cooperative, self-regulation. But Ayres and Braithwaite recognise that, paradoxically, this will usually only come about if the authorities signal a 'capacity to get as tough as needed'. This does not mean issuing threats, or trying to bully companies – both of which are likely to generate 'reactance' and resistance – but it does recognise that 'regulatory agencies', are 'able to speak more softly when they are perceived as carrying big sticks'.[139]

So how might an approach based on 'responsive regulation' be applied to the social media industry, in an effort to get them to act more rigorously against online extremism?

Ultimately, it seems clear that the companies must go beyond responding to complaints and user flagging and implement a system for the identification and instant removal of extremist content, based on a shared database of material. With the afore-mentioned PhotoDNA system, which is aimed at child pornography, images, audio and video are categorised centrally by law enforcement and the technology companies are legally obliged to remove the content. Hany Farid, a computer scientist based at Dartmouth in the US, has worked with the Counter Extremism Project to develop a similar system that would proactively identify extremist photos, videos, and audio clips as they were being posted online – with a view to allowing instant removal. The idea was for the establishment of a similar repository of extremist content, called the National Office for Reporting Extremism, or NOREX.[140]

139 Ibid.; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Regulation Debate* (New York: Oxford University Press, 1992), http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf.

140 Kaveh Waddel, 'A Tool to Delete Beheading Videos Before They Even Appear Online', *The Atlantic*, 22 June 2016; Matthew Reitman, 'How Tech Companies Are Fighting the Digital War Against ISIS', RealClearLife, 7 August 2017, http://www.realclearlife.com/technology/tech-companies-can-fight-online-radicalization-smarter/.

The companies must be pushed to implement such a system as a matter of course. There is a challenge arising from the fact that it is arguably more difficult to define 'extremism' than say, child pornography. And yet, such difficulties are surely surmountable. One area in which government has a critical role to play is in offering a workable definition of 'extremism', which can help inform industry practice. Such a definition will, in general terms, be a priority for the proposed Commission for Countering Extremism – a new body being established to identify and expose examples of extremism. With regards to the online world specifically, a useful starting point for attempts to define extremism would be material which promotes or encourages violence or hatred against groups of people based on a political, religious, racial or ideological cause.

At present, the 'best case' solution of automated, instant removal seems a long way off. In the interim, the authorities can help to decisively alter the trajectory of the debate around these issues, by contemplating a sliding scale of regulatory measures that bring pressure to bear on the corporate giants.

As intimated earlier, the fundamental starting point is that the tech companies must be treated as de facto publishers and distributors of online content. As such, they must take responsibility for their content – or, if necessary, *be made* to take responsibility.[141]

To this end, government might consider the following six-step pyramid of actions, running from bottom to top, which might serve as a tool for leveraging the companies into greater efforts. The aim would be to construct a 'regime' that creates incentives – and where necessary, obligations – for action.

Step 1: Ask the companies to revise and implement more stringent Codes of Conduct/Terms of Service that explicitly reject extremism.

At present, the different tech companies require users to abide by 'codes of conduct' of varying levels of stringency.[142] Twitter bans the posting of material that promotes 'violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease'. Facebook does not allow material that 'directly attacks' people on the same basis. And YouTube prohibits material that 'promotes violence or hatred against individuals or groups' based on the same characteristics. All of the companies prohibit violent threat, or the promotion of violence.[143] This is a useful start-point, but it is clear that they need to go further now in extending the definition of what constitutes unacceptable content.

In May 2016, Facebook, Microsoft, Twitter and YouTube signed up to an EU-sponsored 'Code of Conduct', by which they pledged to establish 'clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content'. They also pledged to review the 'majority of

141 'Responsible Publishing', *The Times*, 1 May 2017, https://www.thetimes.co.uk/edition/comment/responsible-publishing-qllcrnb9h; 'What Facebook knows about you', BBC Panorama, 8 May 2017.

142 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, HC609 (25 April 2017), p. 13.

143 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, HC609 (25 April 2017), § 18.

valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary'.[144]

Such commitments were welcome, but it is clear that there need to be revised, more robust terms of service, which set an industry-wide, robust set of benchmarks. The companies must be pressed to act as a corporate body to recognise their 'responsibility' to prevent extremism as an integral feature of a new code of conduct. The creation of such a code could stand as an important 'test case' for the seriousness and effectiveness of the recently-established 'global internet forum'. The major companies must then be proactive in implementing the new terms of trade. In so doing, they could help effect a sea-change in behaviour, and help to define industry best practice.

Step 2: Require the companies to work with and fund the efforts of an expanded Counter Terrorism Internet Referral Unit (CTIRU)

The CTIRU is based within the Metropolitan Police's Counter Terrorism Command and works with the internet companies to remove online content that incites or glorifies terrorism. More resources should be devoted to the CTIRU, with its operations modeled on the very successful work done by CEOP – which acts as a 'one stop shop' for internet-related issues that impact the safety and security of young people online.[145] An act of good authority on the part of the tech companies, signaling their determination to up their game would be the voluntary negotiation of an agreement by which they agreed to work more closely with, and pay for the services of, the CTIRU. At present, the British taxpayer funds the unit (via the police); yet, its ability to remove online content is wholly dependent on the tech companies.

The Home Affairs Select Committee has proposed that those companies be required to contribute financially for the CTIRU – in the same way that football clubs are required to pay for match-day policing around their grounds. It would be a valuable expression of good intent, for the companies to enter into such an arrangement voluntarily.[146] If a voluntary agreement is not forthcoming, however, then the government should insist that the companies contribute financially towards the work of the CTIRU.

Step 3: Empower the forthcoming Commission for Countering Extremism to oversee content removal online

Clearly, it is sometimes difficult to identify jihadist content when it is coded in Arabic – or even English – but shows no explicit scenes, such as beheadings. One useful remedial step would be the creation of an expert-curated feed of data, which would provide the social media companies with updates on the jihadist content that is being shared.

Such a data feed could be overseen by a sub-committee of the government's proposed new Commission for Countering Extremism – perhaps in liaison with GCHQ. Cataloguing data in this way would cut the lag-time where social media companies have to find (or have

144 'European Commission and IT Companies announce Code of Conduct on illegal online hate speech', European Commission, 31 May 2016, http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

145 For example, *Child Exploitation and Online Protection Centre (CEOP): The Way Forward*, Home Office, Cm 7785 (January 2010), http://dera.ioe.ac.uk/10569/1/7785.pdf.

146 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, HC609 (25 April 2017), § 33.

content reported to them) before they can begin reviewing and removing it.

Alongside this, the Commission for Countering Extremism could work to foster a collaborative ethos between the companies and government more broadly. This could include the sharing of best practice as regards:

- methods of locating content;
- developing systems for receiving and processing reports of extremist content; and
- support for smaller platforms struggling to deal with these issues.

Together, the aim should be to find effective ways of sharing aggregated or anonymised data in a way that allows industry to exploit its access and expertise, in order to understand the jihadist movement in greater detail and identify collective steps which can limit the use of online platforms by extremists.

Step 4: Establish a new independent regulator of social media content, within the purview of Ofcom.

At present, internet content is not within the remit of the independent regulator and competition authority for the UK communications industries, Ofcom. The government should therefore create a new independent regulator – either within Ofcom, or parallel to it. Such a move would be entirely in keeping with the stated goals of Ofcom - to make sure that 'people who watch television and listen to the radio are protected from harmful or offensive material' and that 'viewers of video on demand services are protected from harmful content.[147] This would tend to suggest that Ofcom has an intrinsic interest in expanding its focus to include the tech companies that operate the principal social media platforms.

In line with recent calls for the regulation of internet companies to 'ensure businesses and other organisations are transparent and accountable in respect of child safety, child welfare and children's rights in the online environment', the regulator should set new requirements in terms of accountability and transparency.[148] Social media providers should be obliged to provide: a transparent, accessible process for reporting extremist content; clearly-stated guidelines within which material will be removed (no more than several hours); quarterly reporting on rates of removal; and a commitment to block all copies of extremist material when flagged.

Step 5: Put in place a system of financial penalties, administered by the independent regulator, to force company compliance

The independent regulator should have the power to implement major fines on UK-based subsidiaries of the tech companies, with a view to

147 What is Ofcom?, Ofcom, https://www.ofcom.org.uk/about-ofcom/what-is-ofcom. See Communications Act 2003 paragraphs 4 (h), 4 (j), 13.2 (a); Communications Act 2003, paragraph 319.2 (b) and (e); Communications Act 2003, 319. 6 (b)

148 CHIS Manifesto 2017, http://www.chis.org.uk/2017/04/30/election-2017-a-digital-manifesto.

deterring and changing behaviour. In 2015, Ofcom revised its penalties' guidelines to place an emphasis on deterrence and setting precedents. Ofcom has significant discretion when levying a financial penalty to consider the offender's size and turnover. It also considers the harm caused by, and the 'seriousness' of, the offence in question.[149] These same principles should be considered when establishing a framework for the financial punishment of those internet companies that fail to live up to their responsibilities.

During the past year, Ofcom imposed fines ranging from £65,000 to £42million.[150] The same wide range of discretion could be afforded to its regulation of the UK subsidiaries of tech companies, though it is salutary to note that the German Cabinet has recently agreed to proposals that would fine social media companies up to €50 million (£43m), and individuals up to €5 million, for not deleting 'obviously criminal content' within 24 hours, and other hate speech and fake news within seven days. The companies must also run a 24-hour helpline for concerned users – and report back to complainants on how they handled a given case. The Justice Minister behind the new laws, Heiko Maas has called for an 'end' to the 'internet law of the jungle'.[151] He further argued that legal regulations, of the kind now enacted, were 'the only way to increase pressure on the social networks' and 'make the companies more accountable'.[152]

Within the UK, an alternative model for punitive-backed regulation has been provided by Anna Turley's Private Member's Bill, which was designed to tackle online harassment. This proposed that social media companies would be regulated by Ofcom and fined up to £2m, or 5% of their global turnover, for failing to effectively filter threatening material.[153] If the government is chary of the German model, this framework could be adopted as a basic guideline.

Step 6: Consider ways in which the existing legislation against the distribution of extremist material can be used to prosecute repeat offenders from the tech companies

At present, there are clear injunctions against the distribution and dissemination of pernicious material. The Public Order Act 1986, and the Racial and Religious Hatred Act 2006, make possible the prosecution of those who stir up 'hatred against persons' on grounds of religion, race, or sexual orientation. This includes by 'Publishing or distributing written material… [and] Distributing, showing or playing a recording'. The Terrorism Act 2006 makes it clear that distributing or circulating a terrorist publication, or possessing a terrorist publication with a view to distributing, selling, loaning, listening or seeing it are offences.[154] The Act includes reference to the 'reckless' dissemination of material – in a situation where there was no specific intent to cause harm.

If the tech companies are treated as publishers of extremist content (as many – including even Mark Zuckerberg seem increasingly willing to accept), then it follows that they be subject to prosecution in a context in which they wilfully neglect their responsibilities. In

149 Ofcom Penalty guidelines s.392 Communications Act 2003, https://www.ofcom.org.uk/__data/assets/pdf_file/0017/96101/Penalty-guidelines-2015-Section-392-of-the-Communications-Act-2003.pdf; 'Ofcom's revised guidelines on fines – a new emphasis on deterrence', Simkins LLP, http://www.simkins.com/wp-content/uploads/2016/03/Ent.-LR-Article-Ofcom_s-revised-guidelines-on-fines-12.03.16.pdf.

150 Ofcom Financial penalties imposed for the period 01/04/2016 to 31/03/2017, https://www.ofcom.org.uk/__data/assets/pdf_file/0031/96943/financial-penalties-imposed-for-the-period-01042016-to-31032017.pdf.

151 Cara McGoogan, 'Twitter brings IBM's AI machine Watson on board to fight abuse', *Daily Telegraph*, 23 March 2017, http://www.telegraph.co.uk/technology/2017/03/23/twitter-brings-ibms-ai-machine-watson-board-fight-abuse/; Cara McGoogan, 'Germany threatens to fine social media companies €50m for hate speech and fake news', *Daily Telegraph*, 14 March 2017, http://www.telegraph.co.uk/technology/2017/03/14/germany-threatens-fine-social-media-companies-50m-hate-speech/; 'German parliament approves law to fine social media platforms over hate speech', *Reuters*, 3 July 2017, http://www.reuters.com/article/us-germany-hatecrime-idUSKBN19L0WZ.

152 Guy Chazan, 'Germany cracks down on social media over fake news', *The Financial Times*, 17 March 2017, https://www.ft.com/content/c10aa4f8-08a5-11e7-97d1-5e720a26771b.https://www.ft.com/content/c10aa4f8-08a5-11e7-97d1-5e720a26771b

153 Cara McGoogan, 'MPs threaten to fine Facebook and Twitter £2m over online abuse', *The Daily Telegraph*, 6 February 2017, http://www.telegraph.co.uk/technology/2017/02/06/mps-threaten-fine-facebook-twitter-2m-online-abuse/.

154 Terrorism Act 2006, section 2 (1) (a) and 2 (a); and Terrorism Act 2006 sections 2 (1) (a) & (1) (f).

particular, social media companies that have algorithms that effectively 'recommend' extremist content, or promote it and place adverts on it, could be taken to be in violation of the law and that these companies and their officers could be punished appropriately.

Lawyers have already begun to speculate over the extent to which, if social media companies fail to remove extremist content that has been reported to them, they could be held legally liable for that content – on the basis that they had acquiesced in its publication. The Solicitor-General, Robert Buckland MP, has also suggested that the companies could be opening themselves to charges of having acted in a 'reckless' fashion by allowing the dissemination of material of use to terrorists (see below on this offence).[155]

Targeting Demand: Developing New Legislation

The Current Context

In the effort to reduce the spread of online extremist material, it is also worth considering what more can be done offline – particularly with regards to changing the behaviour of would-be consumers of this content. On the basis that there is a supply and demand for any product – whether physical or ideological – this means trying to reduce demand for online extremism. One obvious way of doing this is to raise the bar in terms of the consequences that accrue for those who view this material.

The UK has long been reluctant to act against so-called hate speech – with good reason, given the commitment to protecting free speech the potential for the abuse of such government powers. The enduring effect of this attitude, though, is that prosecutions have been hard to secure against even the most egregious and marginal purveyors of pernicious communication that results in physical violence. Nonetheless, numerous government ministers have asserted the principle that 'what is illegal offline, is also illegal online too'.[156]

The Home Affairs Select Committee has noted that the legislation relevant for dealing with pernicious material online is fragmented, spread across several different acts of parliament, including the Malicious Communications Act 1988 and the Communications Act 2003. To this are added the numerous provisions of criminal law from the virtual world (see below), which might equally be applied to the online environment. The effect of this is that there is a degree of confusion and lack of clarity about legislative provisions as they apply to online content – all of which has been magnified by the rapid evolution of the social media environment. The CPS has attempted to bring some greater precision to the current context, whilst noting that there is 'no substitute for clearer statutory provisions'.[157]

At present, the legal context for dealing with 'extremism' is framed by several pieces of legislation (see appendix 1 for full details):

155 Alexi Mostrous, 'Facebook publishing child pornography', The Times, 13 April 2017.

156 House of Commons Home Affairs Committee, *Hate crime: abuse, hate and extremism online Fourteenth Report of Session 2016–17*, HC609 (25 April 2017), §26.

157 Ibid., § 53-56.

1) Sections 17 - 29 of the Public Order Act 1986, which criminalises acts intended to stir up 'racial hatred, including by: the 'Use of words or behaviour or display of written material'; 'Publishing or distributing written material'; 'Public performance of play'; Distributing, showing or playing a recording; 'Broadcasting or including programme in programme service'

2) The Racial and Religious Hatred Act 2006, which supplements the 1986 Act above, by adding 'offences involving stirring up hatred against persons on religious grounds'.

3) The Criminal Justice and Immigration Act 2008, which amends the 1986 Act so as to create offences of intentionally stirring up hatred on the grounds of sexual orientation.

4) The Terrorism Act 2000:

- Section 57 makes it an offence to **possess** articles for the purpose of terrorism
- Section 58 makes it an offence to **collect** information useful to committing or preparing acts of terrorism.

5) The Terrorist Act 2006, which created a number of new criminal offences relating to online material:

- direct and indirect encouragement and/or glorification of terrorism (**Section 1**)
- dissemination of terrorist publications (**Section 2**)
- preparation of terrorist acts (including planning)
- training for terrorism, and attendance at places used for terrorist training.

Section 3 of the Terrorism Act 2006 also allows an officer to arrest and charge a person who they believe to be using terrorist-related material on a website that could be understood to be 'direct' or 'indirect encouragement' or "glorification" of a terrorist act.[158]

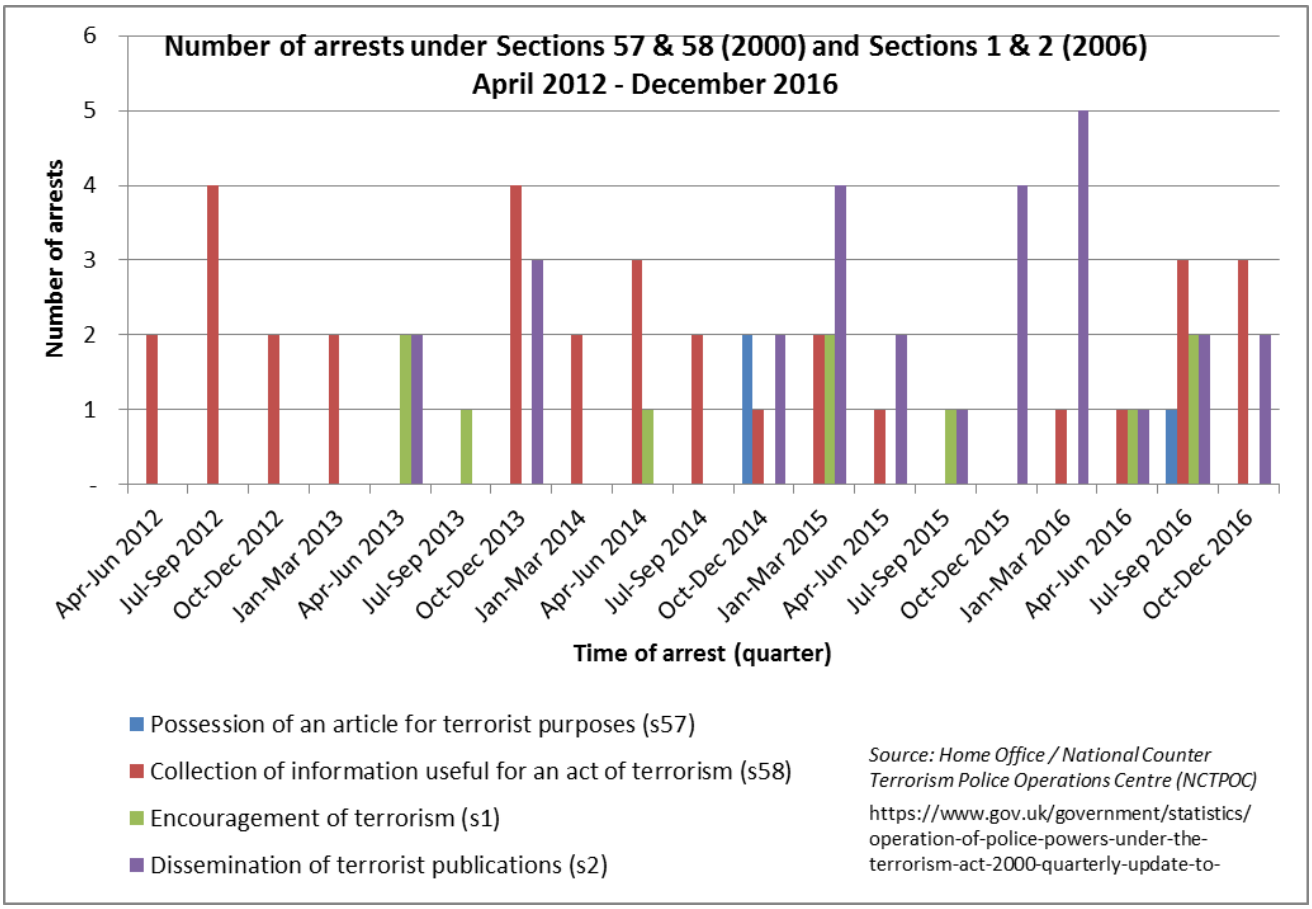
On the basis of the above legislation, there have been a number of arrests and convictions for the possession of materials that are of use to terrorism – as demonstrated in the table and charts below, as well as Appendix 2.

158 Brian Blackmore, *Policing Cyber Hate, Cyber Threats and Cyber Terrorism* (2012)

Data table

Offence description and legislation	Time of arrest (quarter)																		
	Apr-Jun 2012	Jul-Sep 2012	Oct-Dec 2012	Jan-Mar 2013	Apr-Jun 2013	Jul-Sep 2013	Oct-Dec 2013	Jan-Mar 2014	Apr-Jun 2014	Jul-Sep 2014	Oct-Dec 2014	Jan-Mar 2015	Apr-Jun 2015	Jul-Sep 2015	Oct-Dec 2015	Jan-Mar 2016	Apr-Jun 2016	Jul-Sep 2016	Oct-Dec 2016
Possession of an article for terrorist purposes (s57)	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	1	-
Collection of information useful for an act of terrorism (s58)	2	4	2	2	-	-	4	2	3	2	1	2	1	-	-	1	1	3	3
Encouragement of terrorism (s1)	-	-	-	-	2	1	-	-	1	-	-	2	-	1	-	-	1	2	-
Dissemination of terrorist publications (s2)	-	-	-	-	2	-	3	-	-	-	2	4	2	1	4	5	1	2	2

Combined chart



It is clear, however, that convictions for the possession of terrorist-related materials have only been possible where at least one of three criteria are satisfied:

- Intention
- 'Directionality'
- 'Tangibility'

The meaning of the former term is clear. Hence, under section 57 of the Terrorism Act 2000 there has to be a reasonable suspicion that this possession of articles is connected with committing, preparation or instigating an act of terrorism.

By 'directionality', we mean that, possession has only been criminalised in so far as it is aimed at, or distributed to, another individual.

By 'tangibility', we mean that the possession of extremist material has only been criminalised when it has been connected with an act of terrorism, or violence.

The application of these ideas can be seen from consideration of the text and implementation of section 58 of the Terrorism Act 2000. This clearly goes further than section 57, in that there is no requirement for the prosecution to prove that the defendant possessed the information for a terrorist purpose. Instead, the touchstone of this offence is the nature of the information rather than the circumstances in which it is possessed. Nevertheless, it is still required that the information must be of *practical assistance to a would-be terrorist*. The possession of material, which merely glorifies terrorism, is judged insufficient to qualify as an offence, even where it has the effect of encouraging such activity.

The truth of this was confirmed in 2008 when the case of Khalid Khaliq came before the courts. Khaliq's house had been searched in connection with the 7/7 bombers, and he was then charged and convicted on three counts of possessing material contrary to section 58 of the Terrorism Act 2000. Khaliq then launched an appeal that clarified the meaning of section 58, and narrowed its scope – prosecutors now had to prove that the material would assist practically in the preparation or committing of a terrorist act. Consequently, Khaliq was only charged on one count (possession of the Al Qaeda manual).

The consequences of this can be seen, for example, in relation to the *Inspire* magazines published by Al-Qaeda in the Arabian Peninsula. Existing legislation means that it is only articles such as that entitled 'How to make a bomb in the kitchen of your mom' that cross the statutory threshold for criminalisation. Whilst more innocuous articles might help stimulate terrorist activity, they would not be actionable under section 58, if they did not 'provide practical assistance to a person committing or preparing an act of terrorism'. [159]

This limited interpretation of what constitutes 'possession' also applies, *mutatis mutandis* to both the Racial and Religious Hatred Act 2006 and the Terrorism Act 2006. With regards to the latter, the

offence of the 'glorification' of terrorism requires the 'reasonable expectation' that the audience will 'emulate terrorism' in the present (i.e. the 'glorification' could not be merely rhetorical and could not relate to the distant-past).[160] To be used as evidence of an offence, a statement has to be publicly published (in some form – including electronically) – and has to have had an effect on someone consuming it. The publisher must also intend the audience to be directly, or indirectly encouraged to commit, prepare or instigate acts of terrorism – or be 'subjectively reckless' as to whether the public will be so encouraged; it is no defence to show that the intention was unsuccessful.[161]

Section two of the 2006 Act deals with the secondary dissemination of terrorist publications, with intent or recklessness as to direct/indirect encouragement of terrorism. 'Publication' in this context included distribution, circulation, lending and so forth. Possession, *in the context of dissemination*, was also included – but possession *per se*, was not made an offence.[162]

The police have begun to make use of the powers provided for by 2006 Act In 2009, for instance, Shella Roma from Oldham, was convicted of distributing a terrorist publication, and given a three-year community order for seeking to print and distribute an extremist pamphlet called 'The call', which contained an encouragement to jihad.[163] Again, though, the effect of the way in which the law has been implemented has narrowed the meaning of 'possession', to tie it very closely to dissemination; as noted above, possession, in and of itself, has not been challenged.

Section 28 of the 2006 Act offers an alternative model for dealing with materials proscribed by section two of the same instrument. This stipulates that a Justice of the Peace (or sheriff in Scotland), if he/she suspects such extremist materials to be present, can issue a search and seizure warrant. Proceedings for forfeiture can then be taken, with notice given to the owners/occupiers of premises. The latter then have one month to respond; if there is a counter-claim, the case goes to court (either the High Court or a magistrates' court; a Court of Session or sheriff court in Scotland; or the High Court or summary court in Northern Ireland). This process for removing the material – rather than prosecuting the individuals – is modelled on the Obscene Publications Act 1959. In and of itself, it does not alter the fact that possession *per se* is not being challenged – and in any case, it is unclear how effective these powers have been.

Beyond this, the government has backed away from a new Counter Extremism Bill, which, when initially proposed in late 2015, proposed new powers to: ban extremist organisations that promote hatred and draw people into extremism; restrict the harmful activities of the most dangerous extremist individuals; and restrict access to premises which are repeatedly used to support extremism. The bill would have included provision for 'Extremism Disruption Orders' and 'Banning Orders' that might have allowed for an expanded effort to tackle online extremism. In the absence of such initiatives, it is worth asking again what more can be done to deal with this problem.

159 Possession of terrorist materials, 6KBW College Hill, 13 October 2014, http://www.6kbw.com/cms/documents/AJC_Article.pdf.

160 Clive Walker (ed.), *Terrorism and the Law* (Oxford: Oxford University Press, 2011), p. 363-7.

161 Ibid., p. 366.

162 Ibid., p. 368.

163 'Woman sentenced for jihad leaflet', *BBC News*, 20 March 2009, http://news.bbc.co.uk/1/hi/uk/7972580.stm.

Recently, there have been signs that the authorities feel the law is failing to police the online space adequately. Earlier this summer, for instance, the Crown Prosecution Service produced (CPS) new guidelines that aimed to deliver a tougher stance on online hate crime – described as having a 'corrosive effect' on society.[164] 'Hate Crime' can already be prosecuted under the Public Order Act 1986, and the Crime and Disorder Act 1998; it is defined by the CPS as 'any crime perceived by the victim or another person to have been motivated by hostility or prejudice based on a person's race, religion, sexual orientation, disability or transgender identity'.[165] Until now, however, there has been a sense that the law (or rather, its implementation), has failed to keep pace with the evolving social media environment. Discussions about how to resolve this shortfall, inevitably raise many of the same issues as do debates around extremist content more broadly.

At present, much of the responsibility for tackling online extremism falls to the Counter Terrorism Internet Referral Unit (CTIRU), which is based within the Metropolitan Police's Counter Terrorism Command. This unit refers material to investigation teams nationally when it is identified that an offence may have been committed under the Terrorism Act or other legislation; and it removes online content that incites or glorifies terrorist acts under Section 3 of the Terrorism Act 2006. Yet, in light of the foregoing, we need to consider whether it is sufficiently armed to do the job to which it has been assigned? Are additional legislative tools required to tackle extremist content? Is it possible to develop more targeted powers to tackle the possession and consumption of extremist material?

Of course, there is a need for caution here. This was demonstrated in the case of Rizwaan Sabir, a student at the University of Nottingham, who was arrested and detained for seven days in 2008 for downloading al-Qaeda materials. Sabir was subsequently released without charge, when it emerged that the materials were related to his study for an MA and had been obtained from a US-government website. He was paid damages of £20,000 and his case has often been cited as an example of police heavy handedness.

Nevertheless, the scale of the problem facing the security services was made clear in the wake of the Manchester suicide bombing, when MI5 said that there were 3,000 people under active investigation, with another 20,000 persons 'of interest'.[166] It is a source of frustration to many that the majority of perpetrators of terrorism are previously known to the authorities, including to the police and intelligence services. Most are increasingly known to have possessed or consumed extremist or terrorist material online, not all of which meets the current bar for prosecution. At the same time, the increased frequency of attacks and viable plots in the UK and beyond underscores the need to capitalise on opportunities for intervention – particularly when they fall short of the individual preparing to commit an act of violence. It is clear that the authorities do not have all the 'tools' needed to deal with this major challenge. For this reason, new measures to tackle the unlawful possession of extremist material might empower the

164 'CPS publishes new public statements on hate crime', Crown Prosecution Service, 21 August 2017, http://www.cps.gov.uk/news/latest_news/cps-publishes-new-public-statements/.

165 Law Commission, *Hate Crime: Should the Current Offences be Extended? Summary for non-Specialists*, Law Com No. 348 (Summary).

authorities to stop those who have moved a significant way down the path of radicalisation, but are not yet involved in planning an actual attack.

Options for change

a) The development of civil remedies, supervised by the courts, which would treat the possession of extremist material as a form of anti-social behaviour.

Already available on the statute book are anti-social behaviour orders (ASBOs), which can be issued under section 1 of the Crime and Disorder Act 1998. In addition, Criminal Behaviour Orders (CRIMBOs) are issued when a person is convicted of a criminal offence involving persistent anti-social behaviour. In the context of the struggle against radicalisation and extremism, such instruments might be revised in order to deal with those against whom criminal prosecution is neither desirable nor possible.

There are important precedents here. After 9/11, the Anti-Terrorism Crime and Security Act 2001 created the possibility of indefinite detention for non-nationals suspected of terrorism, but who could not be deported. In 2004, this measure was deemed incompatible with the Human Rights Act 1998, by the House of Lords. Consequently, the Prevention of Terrorism Act 2005 created the system of control orders – the initial scheme for dealing with people of serious concern, about whom there was no indictable evidence. 52 control orders were imposed on men suspected of involvement in terrorist activity. They were required to reside in a place of the Home Secretary's choosing (in almost half of cases, this meant involuntary relocation) – and were subject to numerous other restrictions of movement, communication and association.

In 2011, control orders were replaced by Terrorism Prevention and Investigation Measures (TPIMs), 'to protect the public from the risk posed by persons believed to have engaged in terrorism-related activity, but who can neither be prosecuted nor deported'. TPIMs are imposed by Home Secretary, but subject to review in the High Court (in closed session, with special advocates present, but not the subject of the TPIM). They allow for the imposition of various restrictions on individuals deemed to be of serious concern. TPIMS can last for a maximum of two years and initially there was no power of relocation (as there were with Control Orders). Limited locational restraints were, however, reinstated by the Counter-Terrorism and Security Act 2015.[167] Under TPIMs, unlike Control Orders, an individual cannot be denied all access to computers, landlines or mobile phones. Available measures include: curfew; GPS tagging; reporting requirements and restrictions on travel, movement, association, communication, finances, work and study; and limits (but not total prohibition) on internet use. One option for dealing with online extremism would be to expand and extend significantly the use of the TPIMs. To-date these

166 Sean O'Neill, Fiona Hamilton, Fariha Karim, Gabriella Swerling, 'Huge scale of terror threat revealed: UK home to 23,000 jihadists', *The Times*, 27 May 2007, https://www.thetimes.co.uk/article/huge-scale-of-terror-threat-revealed-uk-home-to-23-000-jihadists-3zvn58mhq; '23,000 people have been "subjects of interest" as scale of terror threat emerges after Manchester attack', *Daily Telegraph*, 27 May 2017, http://www.telegraph.co.uk/news/2017/05/27/23000-people-have-subjects-interest-scale-terror-threat-emerges/.

have been used exceedingly sparingly. In the first year of operation, they were imposed on ten men – nine of whom were British nationals who had previously been subject to a control order.[168] It is worth considering whether TPIMs might now be employed more widely and used to target those who possess and consume extremist materials.

Alternatively, the abortive 'Extremism Disruption Orders' could be revived in this context. The value of such civil remedies is that they serve to stigmatise certain kinds of behaviour and hopefully help to drive extremist material out of the mainstream.

b) New legislation to criminalise possession and consumption.

It is worth asking whether we need new legislation to combat specifically the possession and consumption of extremist material. As a start-point, this might read across from existing legislation that criminalises the possession of lewd and indecent images of children. Those possessing indecent photographs of children are charged under the Criminal Justice Act 1988. Section 62 of the Coroners and Justice Act 2009 created a new offence for possession of a prohibited image of a child, with a punishment of up-to three years for those found guilty (six months' imprisonment, or a fine, or both, for those found guilty on summary conviction). The offence was aimed at non-photographic material and for an image to be deemed 'prohibited' it had to be: pornographic; grossly offensive, disgusting, or otherwise obscene; and focused solely or principally on a child's genital or anal region – or portraying a sexual act. The same act defined a pornographic image as one that 'must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal' – with the adjudicating magistrate, judge, or jury to decide whether the threshold had been met. There is a defence of 'legitimate reason' for possession of such images (not defined – and burden of proof on defendant); or that the person had not seen the images – and did not know, or suspect they were indecent.[169]

Could the same kind of provisions not be enacted for dealing with extremist, pro-terrorist material?

One option would be new legislation to criminalise the 'aggravated possession and/or persistent consumption of material that promotes hatred and violence, in the service of a political ideology'.

As the above phrasing makes clear, the goal here would not be to criminalise every individual who stumbles across extremist material online – whether accidentally, naively, or out of innate curiosity. Instead, the offence would by its nature have to be 'aggravated', or 'persistent' – conducted 'in the service of a political ideology'. As with the existing legislative provisions against sending malicious communications online, the offence would require a high evidentiary threshold and prosecutors would not proceed unless there was a public interest in so doing.

167 'Relocation Relocation Relocation', Independent Reviewer of Terrorism Legislation, 24 November 2014, https://terrorismlegislationreviewer.independent.gov.uk/relocation-relocation-relocation/.

168 David Anderson Q.C., Terrorism Prevention and Investigation Measures in 2012, First Report of the Independent Reviewer on the Operation of the Terrorism Prevention and Investigation Measures Act 2011, March 2013, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/first-report-tpims.pdf.

The purpose of the legislation would not be to criminalise, or deter genuine research – but instead to target those whose possession, or consumption of extremist material was nefarious.

Adapting the approach taken towards child pornography, extremist material could be broken down into three distinct categories, with penalties for the consumption/possession of this content weighted accordingly, and with reference to: an offender's own history (including any previous convictions); the volume of material; and the nature of the material. At the lower end, for instance, those found to be in possession of 'category 3' material could be issued with a warning – with legal proceedings enacted only if they refused to dispose of/take down the content.

Those found guilty of more serious consumption/possession offences could be subject to a graduated tariff of sentences, defined by the nature of the material in question:

169 'Prohibited Images of Children', CPS, http://www.cps.gov.uk/legal/p_to_r/prohibited_images_of_children/.

Category 1 – Most Serious	Images of Extreme Violence that include murder, torture, sadism (beheading etc)	*Child Pornography equivalent: Category A: 'Images involving penetrative sexual activity'; 'possession of images involving sexual activity with an animal or sadism'.*
Category 2 – Intermediate	Material that explicitly encourages a resort to violence (for example, calls to physical force/violent jihad); material that explicitly promotes sectarian hatred (e.g. explicit forms of takfiri pronouncement; the articulation of virulent anti-semitism or the denigration of other faiths ("Hindus are excrement" etc)	*Child pornography equivalent: 'Possession of images involving non-penetrative sexual activity'.*
Category 3 – Least Serious	Material that promotes hatred against women and racial, religious or sexual minorities; Material that implicitly promotes a resort to violence	*Child pornography equivalent: 'Images of erotic posing'.*

Based on the fore-going, Appendix 3 offers an outline for the way a sentencing tariff could be constructed.

Part Three: Assessing Public Attitudes

When considering policy options in the struggle against online extremism, it is essential that attention be paid to public attitudes. As noted at the outset of this report, one of the broader challenges we face is the novelty of the issues under review. Debates about how to balance 'security' and 'liberty' have a long provenance – yet they are now being played out in an entirely new technological setting. There is a sense to which the rapid development of social media and other online platforms has raced ahead of society's ability to reach a consensus on how to use them; norms of behaviour and values are still being contested.

It was for this reason that we felt it was important to try and tease out public attitudes on some of the issues arising from our work. A survey of this kind afforded the opportunity to 'road-test' the acceptability of certain premises and policy options – including those discussed in part two – but the aim was not to try and 'pick the policy that is most popular'. Instead, we wanted to try and understand the parameters of public opinion and gain insight into a broader range of views. As the following discussion shows, the survey also allowed us to discern the differences between certain subsets of the population – to identify particular constituencies that hold specific kinds of views on these issues. We hope that this might be of use to those elected officials and civil servants tasked with carrying this agenda forward.

Policy Exchange worked with ICM to test public views on a number of issues connected with online extremism – and various remedies that might be applied to dealing with it. We interviewed a representative online sample of 2,001 GB adults (aged 18+), in the period 14-18 July 2017. Interviews were conducted across the country and the results were then weighted to the profile of all adults.

Respondents were recruited from the ICM NewVista panel of over 175,000 members of the British public, each of whom voluntarily joined up. Each time ICM conduct a nationally representative survey (including this one) potential respondents are sampled in proportion to known population characteristics, including gender, age, region and ethnicity. Non-interlocked quota controls were also imposed on response, to ensure a double lock in the construction of a fully representative geo-demographic sample. Population data for quotas (and weighting) was sourced from the 2011 Census via the Office for National Statistics (in England and Wales), and the General Register

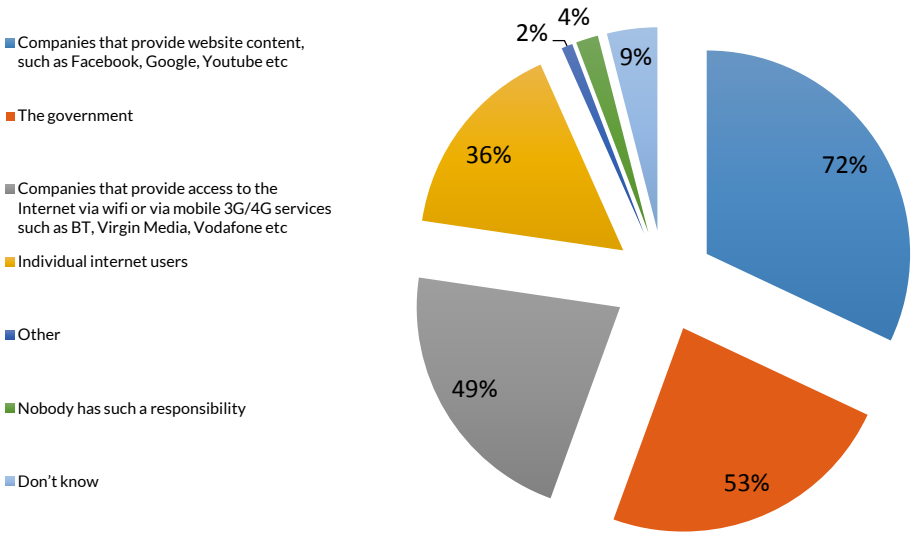
Office for Scotland. Work status information was sourced from the Labour Force Survey.

On this occasion, ICM drew a total of 7,713 records from the panel. Each potential respondent was emailed with a unique link, giving access to their own individual area of the survey on the NewVista protected website. A response rate of 25.9% was achieved, giving a final sample size of 2,001 interviews. Data based on 2,001 interviews is correct to within +/- 2.2% at the 95% confidence interval. The survey was conducted in accordance with ISO protocols for data security (ISO 20001) and ISO 20252 (market research). ICM is a member of the British Polling Council and abides by its rules.

A key focus for our survey was to understand public attitudes about extremist content online and what (if anything) should be done about it. **When asked who was responsible for controlling, or removing, such content (question 10), by far the most popular answer (72%) was 'the companies that provide website content, such as Facebook, Google etc'.**

Respondents could give more than one answer and other popular options were: 'the government' (53%); 'the companies that provide access to the internet (49%); and 'individual internet users' (36%).

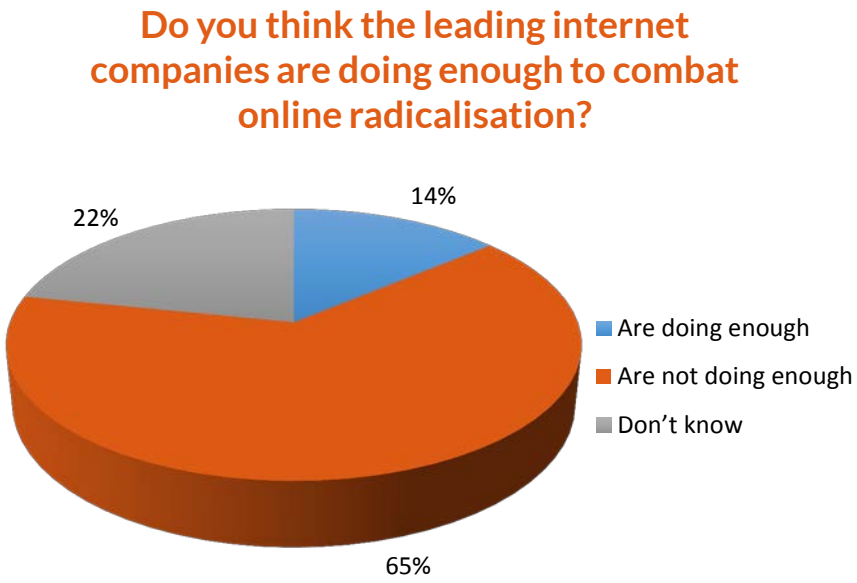
Who has the responsibility for controlling, or removing, extremist content?



In each of these instances, female respondents were more likely than men to state that the companies or the government were responsible for content removal. The eldest cohorts were more likely than their younger counterparts to say this, as were white participants compared to non-white participants. Logically too, those who believed that the internet should be regulated and extremist material removed, were

noticeably more inclined to say that the companies and the government had a responsibility to act.[170]

Furthermore, when asked whether the leading internet companies, such as Facebook, Twitter and Google, were doing enough to combat a process of online radicalisation (see question 11), a clear majority – almost two-thirds of respondents (65%) – answered no.



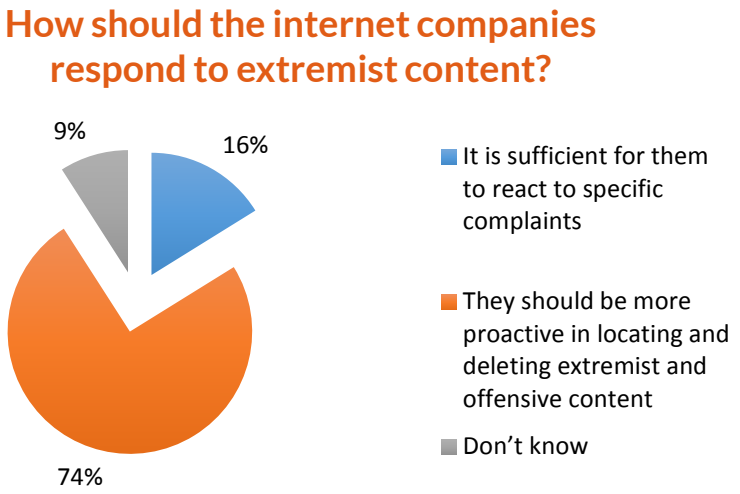
As can be seen, only 14% of respondents were persuaded that the leading internet companies were doing enough to tackle online radicalisation. This fell to just 7% amongst those respondents who took the broadest definition of what constituted extremism: 80% of those who felt this encompassed non-violent hate speech, said that the companies were not doing enough.

Conversely, those respondents most inclined to favour self-regulation of the internet companies were also more likely to agree that the internet companies were doing enough – though it is interesting that even 45% of such people said the companies were not doing enough. And even 39% of those people who felt there should no interference with the internet whatsoever said that the companies were not doing enough.[171]

There was a clear public view that more needs to be done to 'clean up' the online space, when it comes to extremist material. This was confirmed by a further question (question 13), which probed different kinds of approaches taken by the companies. As can be seen below, the results suggest that most people feel the internet companies need to raise their game.

170 Dataset of Polling, available from ICM Unlimited (hereafter, DS), 135-137.

171 DS, 135-137.



74% of respondents stated that the leading players like Facebook, Twitter and Google should 'be more proactive in locating and deleting extremist and offensive content'.

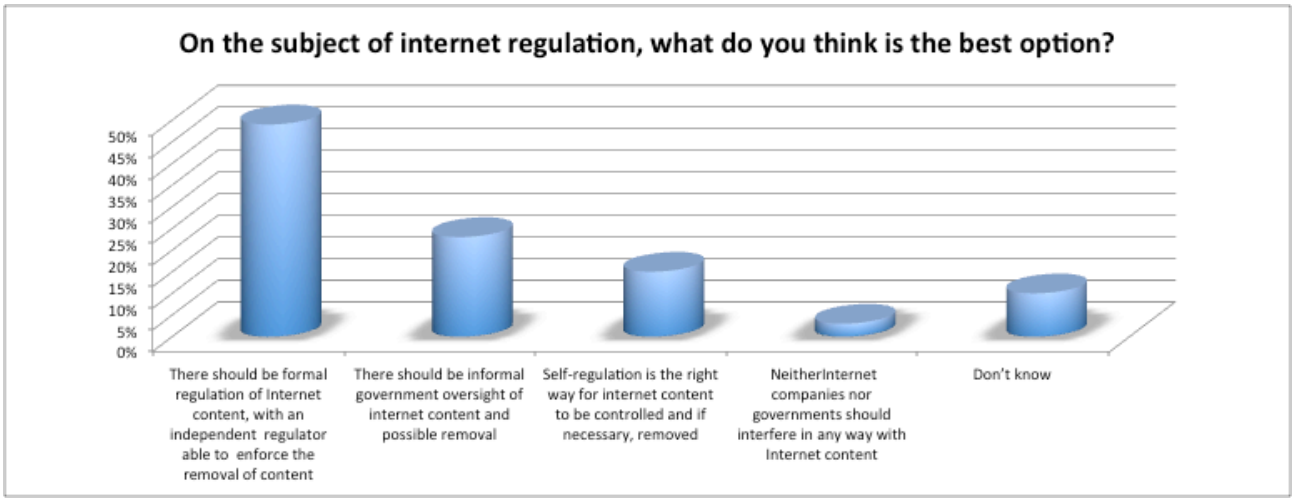
Further analysis shows that this figure rises to 80% when just female respondents are considered; and to over 90% amongst those aged 55 and above. By contrast, just 16% expressed confidence that a more reactive approach was sufficient.[172]

It would seem equally clear that, at present, there is little public faith in the companies to improve their own performance.

When asked for their views on different ways in which the internet might be regulated (see question 12), only 15% expressed support for self-regulation of the kind that currently exists.

23% of respondents said that there should be informal government oversight of internet content, with the provision for content removal – while almost half (49%) favoured formal regulation of internet content, via the creation of an independent regulatory body, which would have the power to enforce content removal.

172 DS, 147-150.



In line with the answers to other questions, those favouring the more robust forms of intervention/regulation were relatively more likely to be: female; older; white; Christian; to have a broader definition of what constitutes extremism; and to feel that the companies were not doing enough to deal with the problem.[173]

From another perspective, 73% of respondents said that there was a 'moral, ethical and social responsibility' on the internet companies to counter extreme narratives on the internet by promoting 'positive alternatives' (70% of people also strongly agreed that the same responsibility devolved upon the government as well). (See question 16).[174]

When asked specifically (question 4a) how extremist material should be dealt with, an overwhelming majority favoured its removal 'as quickly as possible' (78%) from the internet.

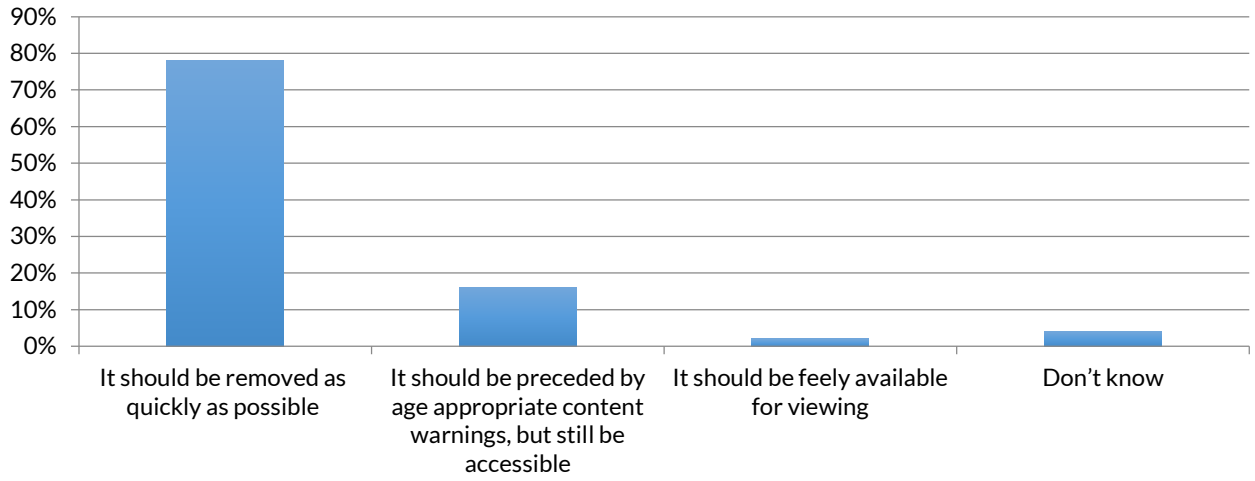
Further analysis shows that female and elder respondents were relatively more likely to endorse such removal. Conversely, those self-identifying as 'non-white' were less likely to give this answer (65% still did so). When results were broken down by religion, Christians were much more likely to favour removal (84%) as compared to those of other faiths (63-66%) or none (73%). And there were also variations according to region of origin.[175]

173 DS, 147-150.

174 DS, 208-314.

175 DS, 46-49.

What is the best way to deal with extremist material on the internet?



At the other end of the spectrum, just 2% of respondents felt that extremist content should be 'freely available' for viewing. An intermediate measure, which might see such material available – but only if accompanied by 'age appropriate warnings' – was the preferred option of just 16% (though men were twice as likely to opt for this as women – 21% as compared to 10% - with a similar pattern evident when one compares the youngest and the eldest cohorts). **What such results underline is the clear preference for greater intervention against extremist material.**

The survey presented respondents with a range of potential measures for tackling online extremism (see question 14) – several of which were discussed in part two of this report. The aim was to establish whether there was an appetite for fresh approaches in this area. **It is striking that there was broad support for all of the measures suggested in part two of this report.**

There was strong support for measures that would use the legal system to put more onus and pressure on the companies to do more. 52% strongly favoured the levying of fines on companies that failed to remove extremist content, with another 26% saying they tended to support this (making for 77% support overall); just 6% expressed opposition to such a move.

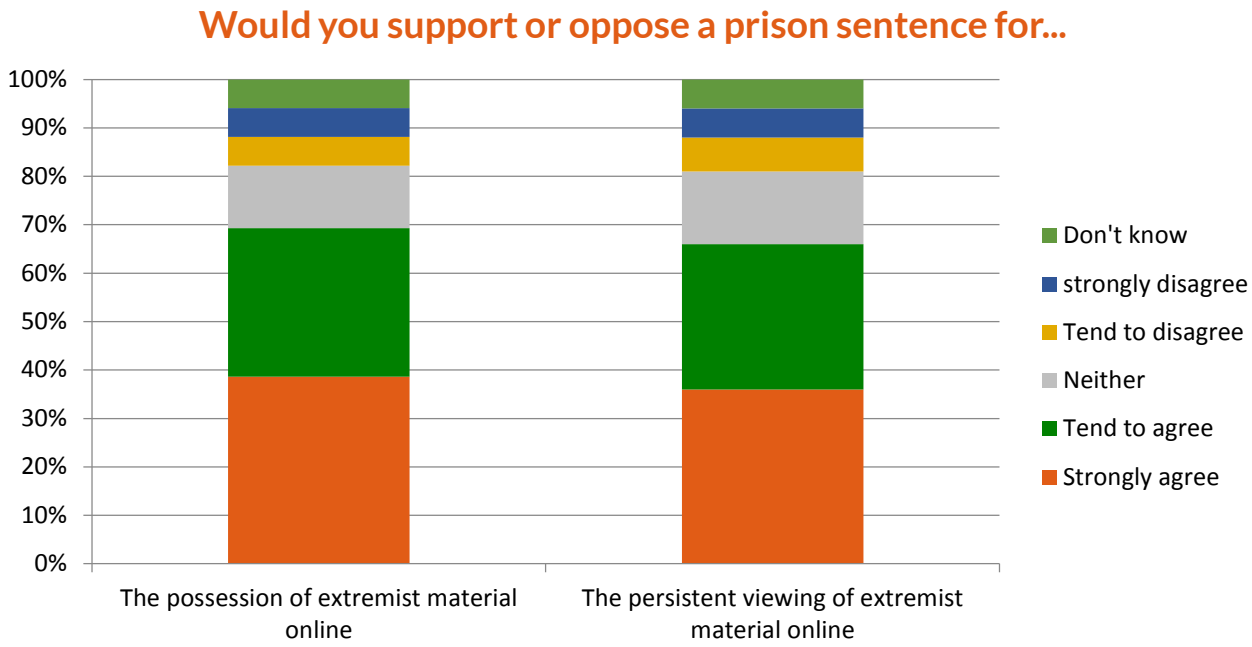
41% of respondents said they strongly supported an independent regulator in the Ofcom mode, with another 34% tending to support such a proposition (75% support overall); just 6% of people opposed this idea.

There was also majority support for both criminal and civil prosecutions of companies and/or their chief executives if they failed to remove extremist content (65% and 64% support in each case, with 11% opposition).

At the other end of the supply chain, (see question 14) there was also strong public support for the idea that new legislation might be enacted to criminalise, respectively, the persistent viewing of extremist

material online, and the possession of such material. In both cases, 46% of respondents voiced strong support for such a proposition with 27/28% stating that they would 'tend' to support it (73-74% support overall). Just 6-7% of respondents said they would oppose measures of this kind.[176]

When questioned further as to whether this meant they would support the handing down of prison sentences for either the possession, or viewing, of extremist material online, a clear majority in each case said that they would, to a greater or lesser extent (70% and 66% respectively – see question 17).[177]

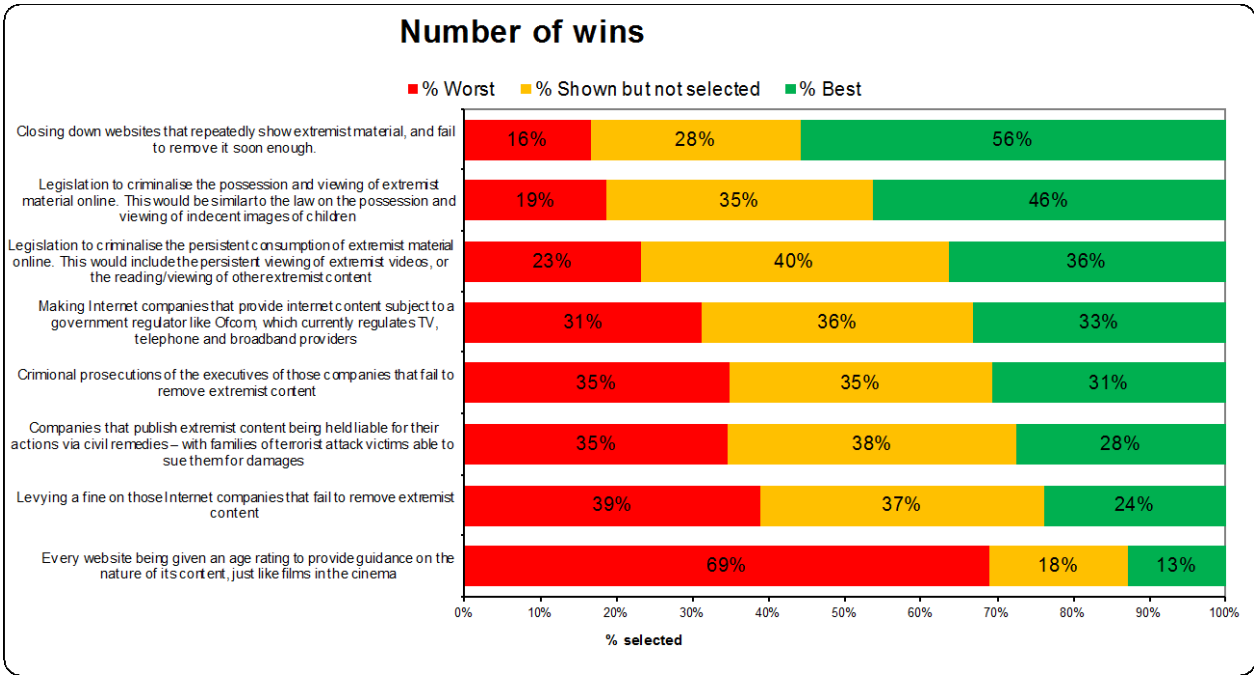


It is noticeable that all of the proposals listed in question 14 garnered majority support (hence, whilst it was the least popular option, some 62% of respondents still supported the idea that every website should be given an age rating).

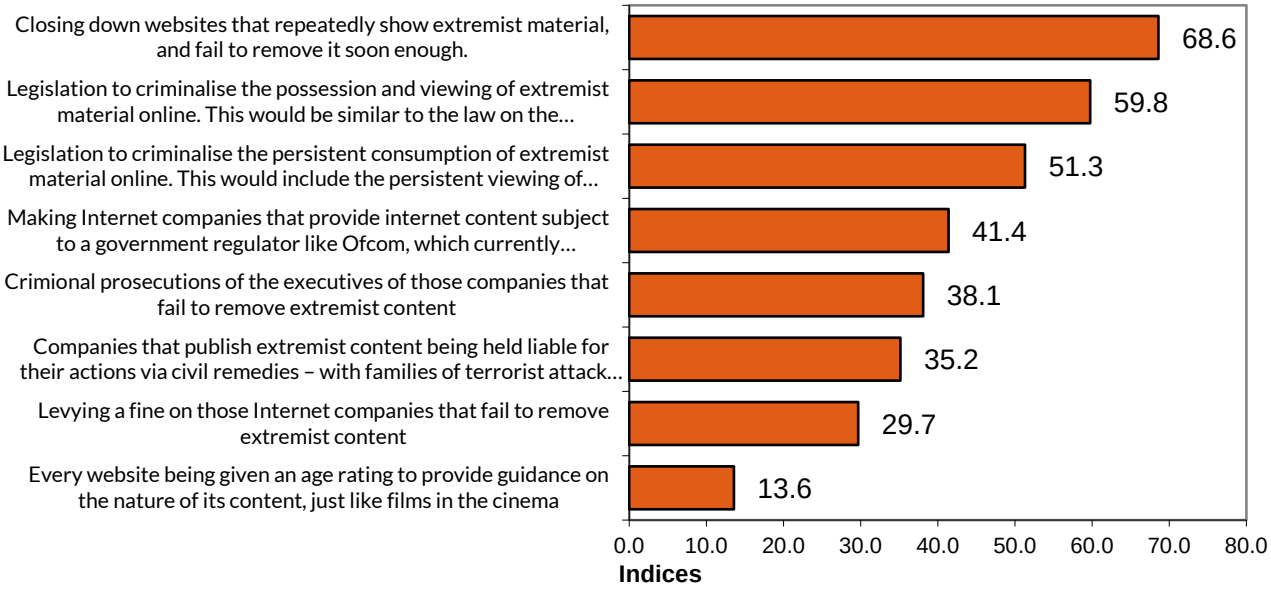
For this reason, our survey also sought to establish preferential views of the proposals, with each ranked in relation to the others. To this end, we offered participants three of the options listed above in a succession of questions, and they were asked to pick the best, the worst (and leave one). We then applied a MaxDiff statistical process to the results, which established a hierarchy of preferences as follows:

176 DS, 151-207.

177 DS, 316-329.



Importance scores



What this demonstrates is that the most popular idea is for websites that repeatedly show extremist material to be shut down: it was 5.1 times more popular than the suggestion that every website be given an age rating.[178] The second and third most popular choices were the propositions for new legislation to criminalise consumption and/or possession. Conversely, when presented as one of a range of options, people were less inclined to choose 'levying a fine' on the companies – perhaps reflecting the view that this is not seen as a particularly

178 60% of people 'strongly' favoured closing down websites that failed to remove extremist content; 80% of respondents supported it to a greater-or-lesser extent.

effective mechanism where large corporations are concerned. Of course, this in itself is no reason to rule out such a step – though it underlines the extent to which such an initiative would need to demonstrate effectiveness in order to win public confidence.

More generally, there is little doubting that the public is fairly convinced of the need for tougher action against online extremism. There are clear majorities for action of one kind or another. By breaking the results down further, we can identify those constituencies where views are the strongest. Analysis of the answers to question 14, as well as the dataset as a whole, suggests that those most in favour of more concerted, government-led action against online extremism, are more likely to be:

1) female
2) elderly
3) Christian
4) have a broader definition of what constitutes extremism – seeing this as encompassing hate speech, as well as physical acts of violence
5) believe that the online space has at least some part to play in the process of radicalisation
6) feel that the internet companies are not doing enough[179]

Further examination of the data thrown up by question 14 also suggests three broad constituencies:

1) Those who believe extremist material online is an important driver of radicalisation, whose definition of that material tends to be broader, and who favour internet regulation and the rapid removal of extremist content
2) Those who are not so persuaded of the importance of online radicalisation, whose definition of extremism is narrower, and who are more skeptical about regulation and more inclined to defer to the companies
3) Those relatively few people who are consistently libertarian in their approach

Of course, there are variations within these three broad schools of thinking, yet the evidence suggests that the former is by some margin, the largest.[180] A majority of people believe that online extremism is a serious problem, driving a process of radicalization into terrorism, and they want something to be done about it.

To delve deeper into the issues surrounding online extremism, our survey sought to probe attitudes on a number of more general questions about the internet, the balance between liberty and security, and the meaning of 'extremism'. It is to these findings that we now turn.

As argued in part two, the government can play an important role in helping to provide a workable definition of 'extremism'. Skeptics often

179 Based on cross-reading of entire dataset.

180 DS, 114-154.

argue that such a definition is unachievable – that to label something 'extreme' is always a value judgment.

Of course, there is an element of truth in that – and in trying to provide a definition, one is inevitably drawn to US Supreme Court Justice Potter Stewart's famous reflection about hard-core pornography, 'I know it when I see it'. There is an intangible dimension to labelling something 'extreme', which means that it defies easy explication. And yet, what Stewart was getting at was the fact that there *is* a 'core' essence of something that we consider unacceptable/problematic – even as there remain ambiguities at the margins. Few would disagree that there can and should be controls on pornography – and though there are grey areas, the red lines are fairly well understood.

With regards to online extremist content, our results suggest that one can make a similar case. **A majority of people consider acts of violence – or the incitement of it – to be 'extreme' (see question one). This is most obviously so, with regards to hate speech that directly encourages violence: 79% of respondents said this was extreme.**

There is, it should be noted, some variation in attitude on this issue according to age. Elder cohorts were more likely than their younger counterparts to say that hate speech encouraging violence was extreme – though, interestingly students, as a group did not fit this trend, with 84% replying that they agreed this kind of hate speech was extreme. Ethnicity was another factor of significance: while 81% of those identifying as 'white' said such hate speech was extreme, just 68% of 'non-whites' did the same. Demarcation by religion and region also revealed differences in outlook, but overall, it seems evident that a clear majority of the population classed hate speech that encouraged violence as 'extreme'.[181] The same pattern was observable – at a lower level – with regards to hate speech which did not 'directly encourage' violence, and which was also labelled 'extremist' by a clear majority (61%).[182]

181 DS, 22-25.

182 DS, 26-29.

Q1. Would you class the following kinds of material as extreme or not?

BASE: all respondents (2,001)	Extreme	Not extreme	DK
Hate speech, which directly encourages people to commit acts of violence	79%	9%	12%
Content showing most serious acts of violence, such as rape or murder	76%	10%	13%
Online trolling/bullying/insults	72%	16%	12%
Hard core pornography	68%	18%	14%
Hate speech, which doesn't directly encourage people to commit acts of violence	61%	24%	15%
Content showing lower level acts of violence, such as assault	58%	28%	14%
Content showing acts of violence in an apparently humourous way, such as in cartoon form or with jokes/music accompanying it	39%	45%	17%
Content supporting hard right or hard left political views	37%	45%	18%
Fake news	37%	46%	16%

As the above summary table of results shows, content showing the most serious kinds of violence such as rape and murder was judged to be extreme by 76% of respondents. 58% also thought that lower level violent acts such as assault should be considered extreme.

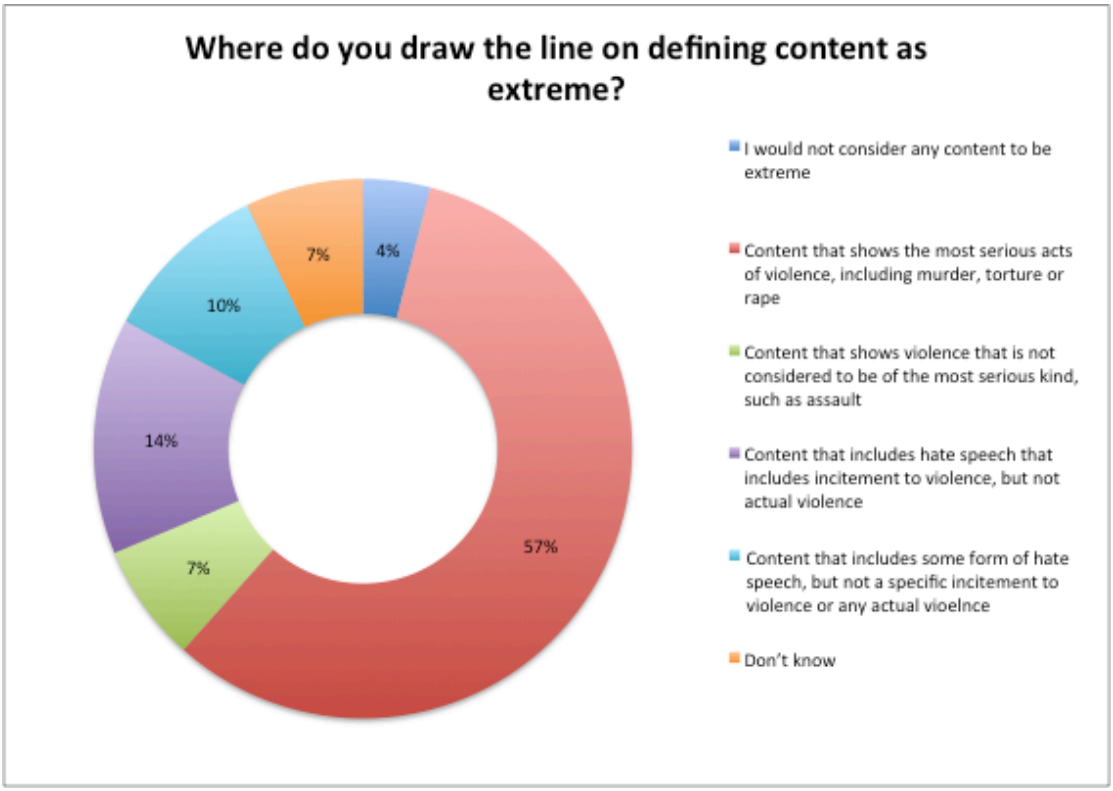
People were far less convinced that satirical content could be considered 'extreme' (only 39% did so – though interestingly, women were relatively more likely to say this, as were younger cohorts/students).[183] Likewise, a majority of respondents did not think that material reflecting strong political views (of the hard left or hard right), should be considered 'extreme' (less than 40% did so – and this figure fell even further in certain regions of the country such as Scotland and the North East).[184]

Still, a degree of vagueness of what constitutes 'extremism' can be seen from the fact that almost as many people would put online bullying/trolling/insults in that category (72%), as would put serious acts of violence like rape, or murder (76%). Such a result tends to underline the paucity of our vocabulary when it comes to discussing content that we deem objectionable.

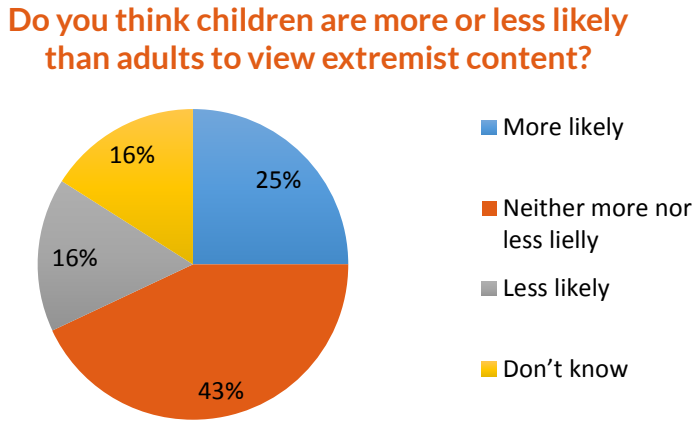
With that said, the line of acceptability/unacceptability for most people (57%) is the point at which content includes the most serious kinds of violence such as rape, or murder (see question 2). Another 7% would draw the line in such a way as to include lesser kinds of violence (e.g. assault). Almost a quarter of respondents, meanwhile, take a much broader definition, and include acts of hate speech that either incite violence (14%) or do not incite violence (10%). Only 4% of respondents said that they did 'not consider any content to be extreme'.

183 DS, 10-12.

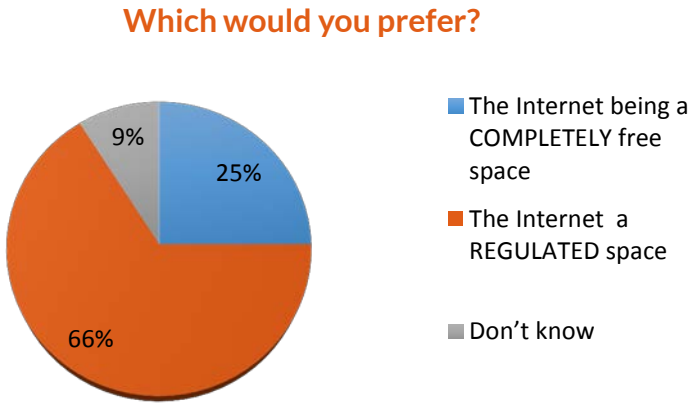
184 DS, 1-3.



The challenge posed by extremist material online was evidently felt to be one that impacted society as a whole. When questioned as to who was more vulnerable to such content, it is notable that only a quarter of respondents (25%) said children were 'more likely' to view it. By contrast, a plurality of 43% said that children were no more likely than adults to encounter this material – suggesting that this is seen as an 'all of society' issue, not merely one of 'safeguarding' young people (see question 18).



Crucially, our survey shows that there is a clear appetite, in general terms, for the regulation of the internet. **Two-thirds of respondents (66%) said that they believed the internet should be a 'regulated space' in which 'extreme material… should be controlled'. By contrast only 25% of respondents said that the internet should be a 'completely free space without any limits on free speech'.**



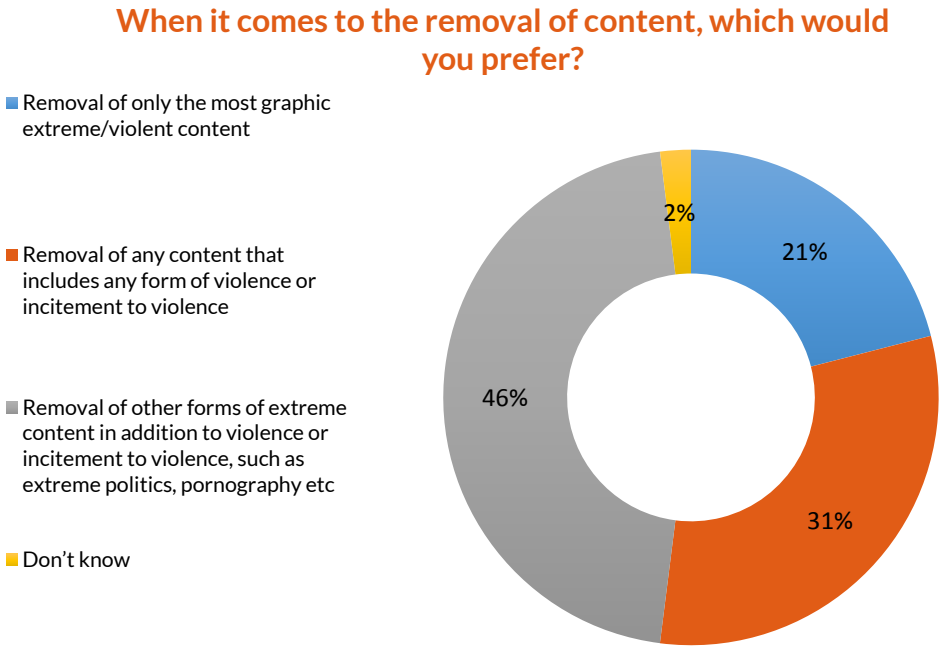
When these results are broken down by different variables, interesting points of divergence emerge. Men, for instance, are significantly more likely than women to support the idea that the internet should be a 'completely free space' (37% as compared to 13%); conversely, four-fifths of women (79%) favour a regulated internet, as compared to just over half of men. Age also makes a difference (the older the respondent, the more likely they were to favour regulation, with 87% of the 65+ group doing so); and so does ethnicity (non-white respondents were markedly less keen on regulation than white respondents – 54% as compared to 68%).[185]

When respondents were classified by religion, there was a clear gap between those of a Christian faith and those not: whereas just 20% of the former endorsed the idea of the internet as a completely free space (and 74% backed regulation), this rose to 40% for Muslims (just 45% backed regulation) and 37% for 'other' faiths (54% favoured regulation). On top of this were regional variations – and, as one might expect, significant differences according to an individual's views on the nature of online extremism.[186]

At the abstract level, therefore, there is evidently an appetite for greater controls on the internet. Moreover, when those respondents in favour of regulation were further asked on what sort of material they wished to see removed (see question 4b), a clear plurality of this sub-group (46%), said that they favoured all material that included violence, incitement to violence, extreme politics and pornography. A majority certainly favoured the removal of all material that crossed the higher threshold of being either violent, or inciting violence (52%).

185 DS, 42.

186 DS, 43-44.



On this issue, interestingly, there is again a particularly marked gender distinction. A majority of women (54%) who favoured a regulated internet preferred the higher threshold of removing sub-violent content – as compared to just 35% of men. Similarly, age differentials showed that a majority of those aged 55 and above preferred the broadest threshold. By contrast, the comparative figure for the youngest cohort (aged 18-24) was just 18%. 45% of the youngest cohort preferred to remove only the most graphic and violent content (as compared to just 21% of respondents overall).[187]

In an effort to further tease out underlying public attitudes, respondents were asked (question 5) to rate themselves on a scale of 1-7, which reflected the degree that they prioritised 'freedoms' or 'security'. Of course, this is necessarily an artificial exercise, but the results are nonetheless suggestive of how people think about these values.

The clear trend of the results shows that the majority of people favour security over liberty. 56% of respondents gave answers of between '5' and '7'. 21% offered the 'neutral' response of '4', while just 18% positioned themselves as '1' and '3'. It is striking that just 3% of respondents came out in favour of 'complete freedoms' – as compared to 17% who said they preferred 'complete security'.

187 DS, 50.

On a scale of 1 – 7, where 1 means that you fully priortise your freedoms over security, and 7 means you fully priortise security over your freedoms, where would you place yourself on that scale?

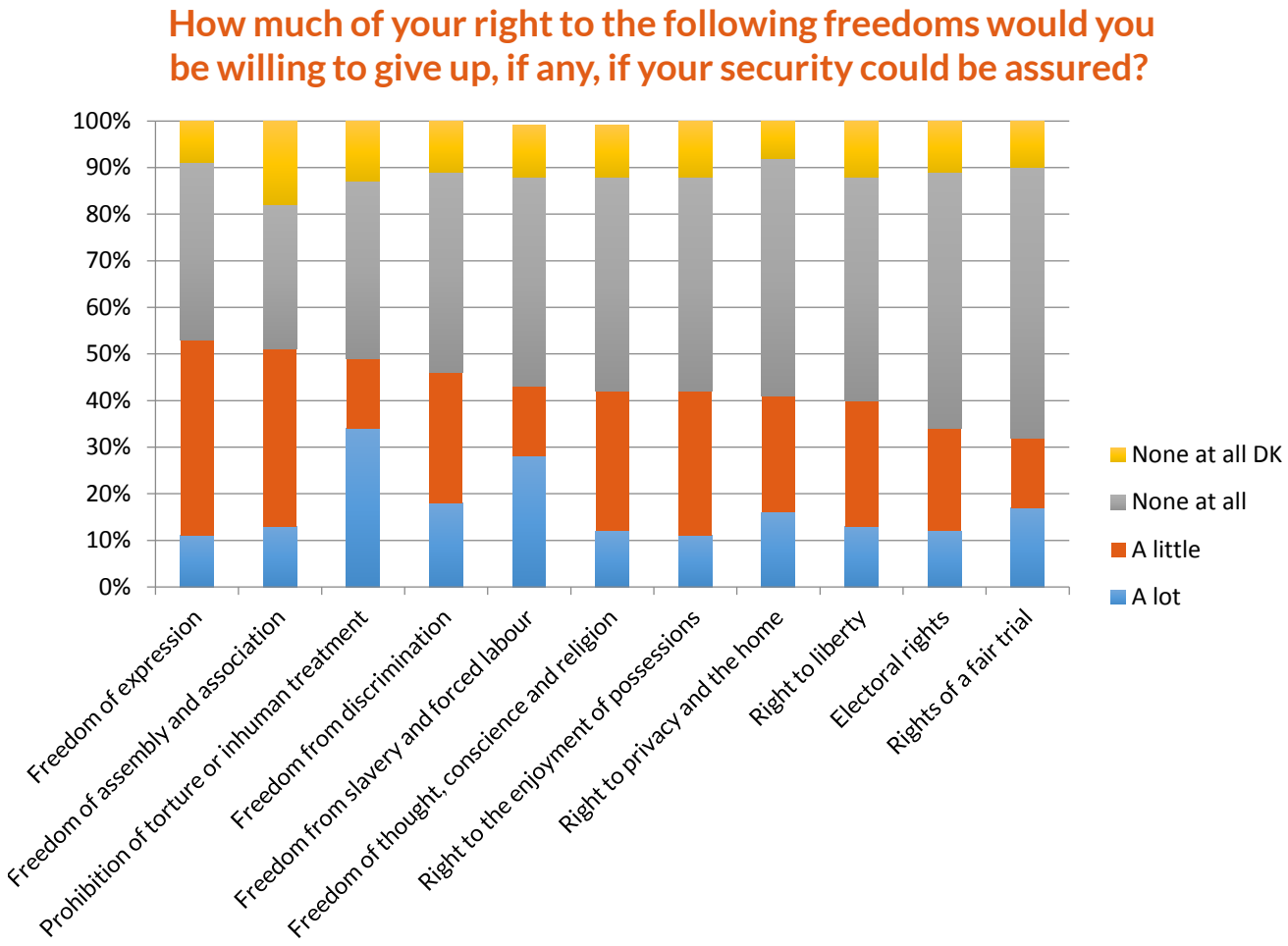
1	2	3	4	5	6	7	DK
3%	7%	9%	21%	24%	15%	17%	5%
← Complete freedoms NET: 18%			Neutral 21%	Complete security-> NET: 56%			

A deeper analysis of these results shows:

- Women are more likely than men to rate themselves at the 'security' end of the spectrum. 64% of female respondents gave scores of 5-7, as compared to 48% of men
- Older respondents were more likely to give themselves a higher score (i.e. to favour security).
- Christian respondents were more likely than others to rate themselves between 5 and 7 on the spectrum (i.e. at the 'security' end).[188]

For those respondents who had not indicated a commitment to complete freedoms (97% of respondents), our survey then sought to establish which liberties people would be willing to give up – and in what proportion – if it meant assuring their personal security (see question 6). Again, it is worth emphasising the artificiality of the exercise – presenting participants with a binary choice, which is in many ways a false choice. Even so, the results afford further insight into public thinking about these critical issues and are fascinating in a number of ways.

188 DS, 54-60.



A majority of respondents said they would be ready to sacrifice – to some degree – 'freedom of expression' (52%), or 'freedom of assembly and association' (51%). Strong pluralities, meanwhile, were prepared to countenance a loosening of the prohibition on torture, or inhuman treatment (49%); or the erosion of freedom from discrimination (46%); or freedom of thought, conscience and religion (43%). For the most part, when asked to choose between giving up a particular freedom 'a lot', or a little', respondents were more inclined to say the latter – though important exceptions to this were on the 'prohibition of torture or inhuman treatment' and 'freedom from slavery and forced labour. In those cases, 34% and 28% respectively said that they were prepared to sacrifice these 'a lot' (as compared to 15% who in each case said they would sacrifice them 'a little').

At the other end of the spectrum, there were three instances in which a majority of respondents said that they would not countenance any derogation of their freedoms: the right to privacy and a home (51%); electoral rights (55%) and the right to a fair trial (58%). Our survey suggests that these are the civil rights most treasured by the British public.

Closer analysis of these results shows numerous interesting variations depending on how one breaks down the data. For instance, female respondents were more likely than men to say they would sacrifice some 'freedom of expression' (56% versus 49%). Conversely, male participants were more likely than women to sacrifice some 'freedom of thought, conscience and religion' (46% versus 40%). Categorising the data according to the age, ethnicity, religion and region of a given respondent also produces a number of points of divergence. For example, with regards to the latter – as one might expect, participants in London – who are perhaps more conscious of the security threat – were usually more ready to countenance a loss of freedom/rights, for the sake of security. By contrast, those in the South West and also the West Midlands were, on a number of issues, less willing than the population as a whole, to make such a trade-off.

Cross-referencing answers to this question with other expressed attitudes throws up additional points of note. Those participants who had stated, in answer to question two, that 'they did not consider any content to be extreme' – which might otherwise be considered quite a libertarian posture - were actually far more likely to be willing to sacrifice: some 'freedom of thought, conscience and religion' (73% said so, compared to 43% of the population overall); as well as 'freedom of expression' (61% versus 52%); and 'freedom of assembly and association' (71% versus 51%). The same pattern was also observable for all other rights/liberties.

Another cohort who were more likely than average to entertain a derogation of certain rights, were those who felt the internet companies were doing enough to combat online extremism. 65% of people in this category, for example, said they would sacrifice some 'right to privacy and the home' in return for security – compared to 41% people overall. Likewise, on the 'right to liberty', 63% of this cohort gave such responses, compared to 40% overall. And the same pattern was evident for those who had answered that 'extreme material should be freely available on the internet'. By contrast, those participants who offered the broadest view of what constitutes 'extremist' material (as inclusive of non-violent hate speech), were simultaneously more likely to say that they would not sacrifice any given freedom/right in return for security.

Trends of this kind are somewhat counter-intuitive as it might have been assumed that those people adhering to a narrower definition of extremism would have also been more likely to favour freedom in general terms; yet, the reverse appears to be true.

The most committed libertarians, meanwhile, were those who believed there should be no external interference (from government, or even independent regulators) over the internet. In every case, they were much more likely to state they were unwilling to sacrifice any liberty for personal security.

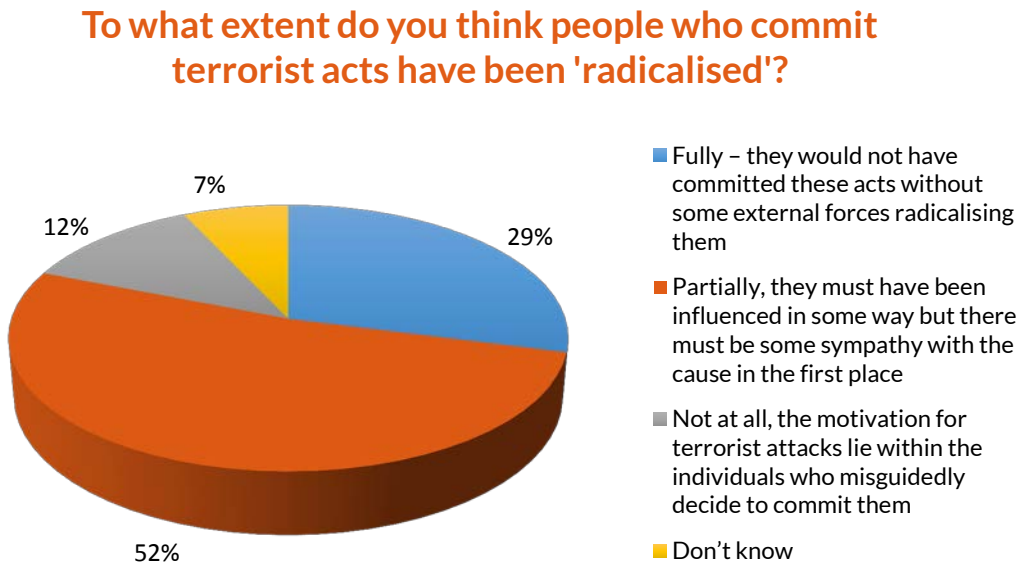
In this way, this question shows the complex, often paradoxical nature of public attitude towards these issues.[189] And yet, taken as a whole, the results from this part of the survey do clearly suggest that, in general terms, people value security over freedom – and it is striking

189 DS, 61-105.

that freedom of expression and a prohibition from torture are taken most lightly.

Given that the debate around online extremism is closely linked to concerns about radicalisation, our survey also sought to gauge public understanding of this phenomenon.

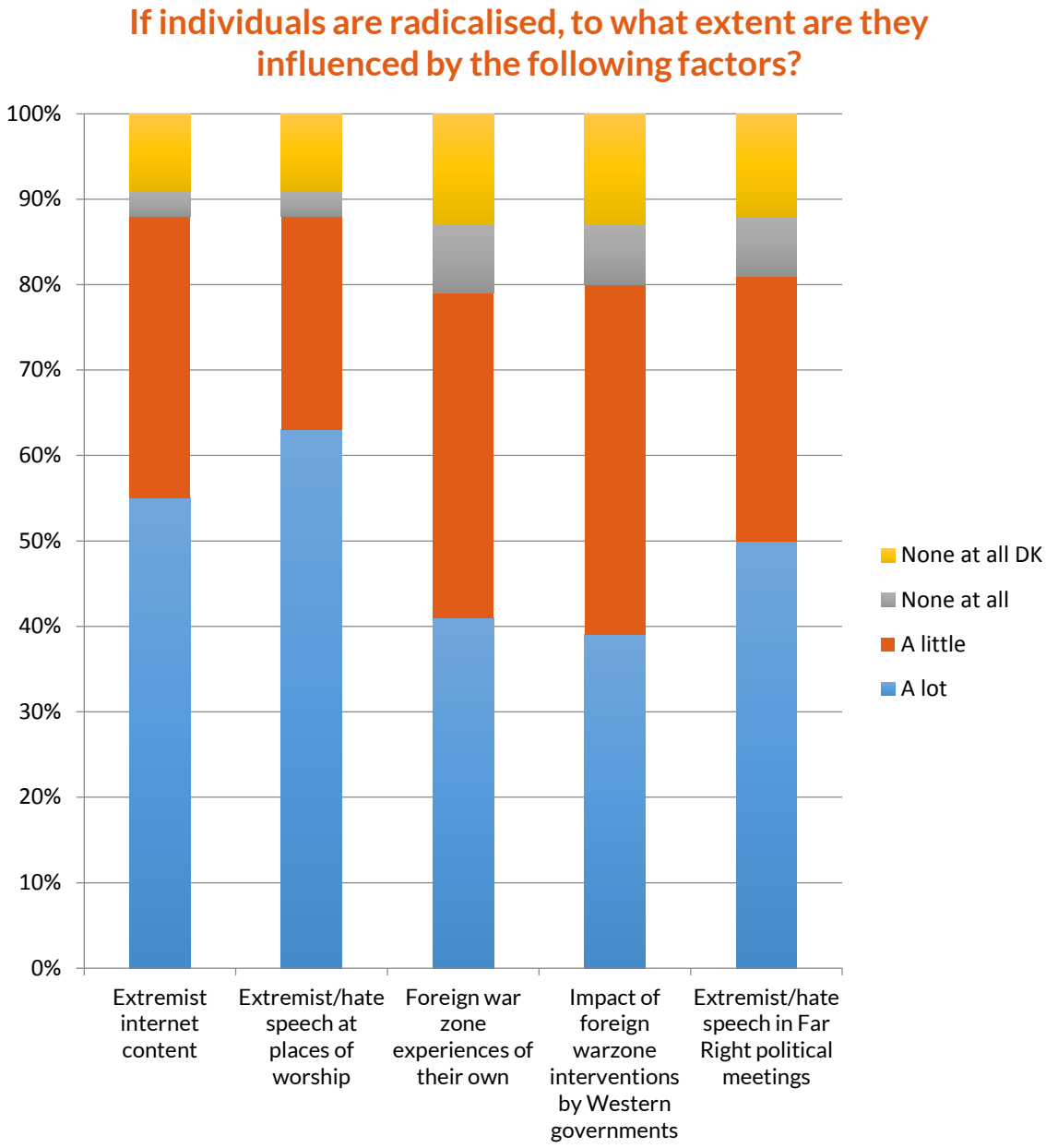
When asked about the reasons why terrorism occurs (question 7), an overwhelming majority of respondents (81%) felt that a process of 'radicalisation' played a critical role. 29% said this was, in effect, the sole driver, with a further 52% stating this was at least partially to blame.



With regards to the actual causes of radicalisation, the picture was less clear. When presented with a list of possible drivers (see question 8), in each case a clear majority of respondents said these were at least 'a little' to blame (and usually 'a lot' to blame). The two factors on which there was the most consensus were:

- 'extremist/hate speech at places of worship', which 63% of people felt was 'a lot' to blame for radicalisation, and a further 25% said was 'a little' to blame;
- 'extremist internet content', which was said by 55% of people to be 'a lot' to blame, while 33% said it was 'a little' to blame'.

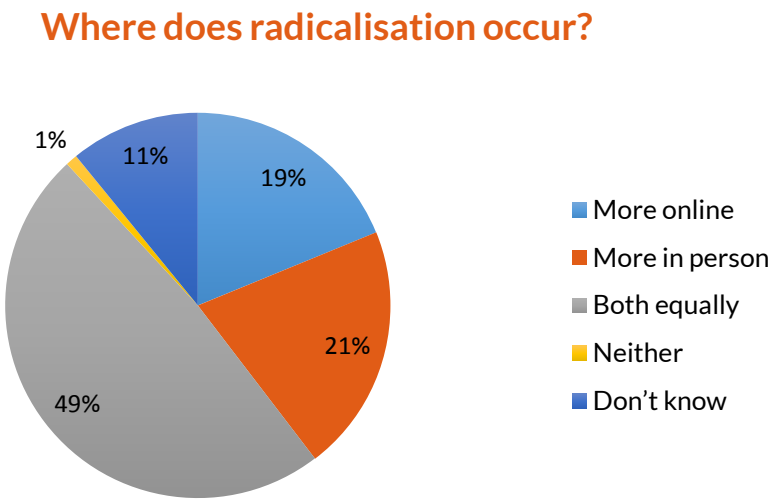
In each case, only 3% of respondents said that neither of these factors had anything to do with radicalisation.



On 'extremist internet content', female participants were significantly more likely than male respondents that this had 'a lot' of influence in the process of radicalisation (62% versus 48%) – though the proportions saying it had some influence were roughly equal. By contrast, there was a more pronounced divergence when results were broken down by age cohort, with elder respondents more likely than their younger counterparts to state that extremist internet content impacted radicalisation.[190]

Overall, though, it seems clear, that radicalisation is seen as something that happens online as much as it happens in person (see question 9).

190 DS, 110-114.



Almost half of respondents (49%) believed that radicalisation was an equal product of both online and offline experiences. 19% said that radicalisation happened 'more online', while 21% said it occurred 'more in person'.

As above, women were more likely to accord a role to the internet: just 14% of female participants said radicalisation happened 'more in person', whereas 73% said it took place either 'more online' or 'equally' on and offline – as compared to 68% of respondents overall.[191]

The cross-comparison of answers to different questions is suggestive of the way in which certain perceptions reinforce one another. As might be expected, those respondents who had said – in answer to question 4a – that extremist material should be permitted to stay online, whether freely, or with an age warning, were more inclined to say that radicalisation took place 'more in person', and to downplay the role of the internet. The same was true of those who felt that the internet companies were doing enough to combat radicalisation online, or those who favoured no government interference/regulation. In many ways, this is not surprising. If an individual believes radicalisation takes place offline, they are obviously less inclined to see the online space as requiring more intrusive forms of control.[192] Even so, it is useful to note the way that certain attitudes reinforce one another.

191 DS, 131.

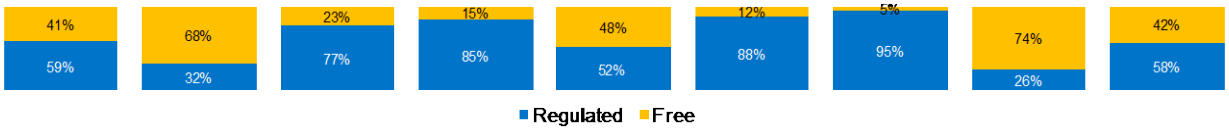
192 DS, 133.

In order to explore further the way in which different attitudes coalesce to produce particular opinions on the question of online extremism, we subjected the data produced by the survey to CHAID analysis. This is an exploratory method that is used to study the relationship between a dependent variable and a series of predictor variables. For present purposes, the chosen dependent variable was, whether or not the internet should be a completely free or regulated space (question 3). By cross-referencing answers to this question with a number of predictor variables, we were able to segment the public into nine different groups, each with varying views on internet regulation. The nine groups we labelled as follows:

- Innocent Internet Libertarians
- Free Space Extreme Content Searchers
- Divided Extreme Content Searchers
- Innocent, Confused Regulators
- Dangerous Internet Environment Regulators
- 'People are the Problem' Believers
- Whatevers
- 'Wild West Sheriffs'
- Blame Culture Interventionists

There is not the space here to analyse how each of these groups breaks down – but the full results can be observed in the dataset. The following table offers a kind of 'family tree' of the attitudes/beliefs that lead people to believe that the internet should be regulated:

<table>
<tr><td colspan="10">Total
1744 (100%)
Regulated = 72%</td></tr>
<tr><td colspan="2">I would think about looking for extremist violent content
497 (29%)
Regulated = 57%</td><td colspan="8">I would never think about looking for extremist violent content
1247 (72%)
Regulated = 78%</td></tr>
<tr><td rowspan="3">People do not radicalise other people, the Internet does
447 (26%)
Regulated = 59%</td><td rowspan="3">People radicalise other people, the Internet doesn't
50 (3%)
Regulated = 32%</td><td colspan="6">Internet providers get a bad press but it's their fault other people post extreme content on their websites
1145 (66%)
Regulated = 82%</td><td colspan="2">Internet providers get a bad press but it's not their fault other people post extreme content on their websites
102 (6%)
Regulated = 42%</td></tr>
<tr><td colspan="3">There is not a moral, ethical and social responsibility for government to counter extreme narratives on the Internet with positive alternatives
666 (38%)
Regulated = 75%</td><td colspan="3">There is a moral, ethical and social responsibility for government to counter extreme narratives on the Internet with positive alternatives
479 (28%)
Regulated = 91%</td><td rowspan="2">The problem with the Internet is not that likeminded people can get together to reinforce their extreme views
50 (3%)
Regulated = 26%</td><td rowspan="2">The problem with the Internet is that likeminded people can get together to reinforce their extreme views
52 (3%)
Regulated = 58%</td></tr>
<tr><td colspan="2">People do not radicalise other people, the Internet does
563 (32%)
Regulated = 79%</td><td rowspan="2">People radicalise other people, the Internet doesn't
103 (6%)
Regulated = 52%</td><td rowspan="2">The Internet has not become like the Wild West
299 (17%)
Regulated = 88%</td><td rowspan="2">The Internet has become like the Wild West
180 (10%)
Regulated = 95%</td></tr>
<tr><td>The problem with the Internet is not that likeminded people can get together to reinforce their extreme views
399 (23%)
Regulated = 77%</td><td>The problem with the Internet is that likeminded people can get together to reinforce their extreme views
164 (9%)
Regulated = 85%</td></tr>
</table>



At one end of the spectrum are the small group of libertarians (just 3% of the population), who are most favourable towards the internet being a free space, based on the fact that:

- They themselves would never consider looking for extreme content
- They do not blame the internet providers for the existence of such content
- They do not see the internet as an incubator for extremism
- At the other end of the scale is a larger group of interventionists (17%) who go nearly all in on internet regulation, on the basis that:

- They themselves would never consider looking for extreme content
- They blame the internet providers for the existence of such content
- They want the government to intervene

The other groups lie somewhere between these poles and their answers to different questions betray a range of quirks. For example, 'Wild West Sheriffs' strongly favour regulation because they blame the internet providers for the existence of extreme content, which they think has helped make the internet like the 'Wild West'; however, on a number of other questions they diverge from the more strident 'blame culture interventionists'.

Finally, it should be noted that our survey threw up some further interesting results that perhaps require a comment. Though it was not a primary focus of this research, there was a clear divergence between respondents self-identifying as 'Muslim' on the one hand, and those adhering to other religions or no religion on the other. For example, on question one, Muslim respondents were relatively less likely to say that content showing acts of violence – at either the most serious, or 'secondary' level – constituted extremist material (51% of Muslims thought lower level acts of violence were extremist, as compared to 58% of respondents overall; just 48% of Muslims thought more serious acts of violence were 'extreme' as compared to 76% overall).[193]

The same was true with regards to hate speech, whether it directly encouraged violence, or not. 52% of Muslims said that hate speech encouraging violence was extreme (as compared to 79% of respondents overall). 43% of Muslims said hate speech that did not actually encourage violence was extreme (as compared to 61% overall).[194] Indeed, with regards to all types of content raised in question one, Muslims were less likely than the overall population to define it as 'extreme' – except on the matter of 'fake news'. Whereas 37% of all respondents defined this as 'extreme', 41% of Muslims did so.[195]

As the results from question 3, mentioned above, show, Muslim respondents were more 'libertarian' in their views about whether or not the internet should be regulated: 40% said the internet should be completely free (compared to 25% of the population overall), whereas just 45% favoured it being a regulated space (compared to 66% overall).[196]

Conversely, however, in their answers to question 5, Muslim respondents were invariably more willing than the population as a whole, to sacrifice some freedoms, in return for personal security. On 'freedom of assembly and association', for example, 70% of Muslim participants said they would give this up a lot or a little, in return for security, as compared to 51% of respondents overall; 57% of Muslims said they could sacrifice the 'right to a fair trial', as compared to 32% of people overall.[197]

193 DS, 11-16.

194 DS, 18, 21.

195 DS, 27.

196 DS, 33.

197 DS, 47-77.

On question 14, meanwhile, Muslim participants were significantly less likely to voice support for a given measure to counter online extremism than their counterparts from other religions, or none. They were also more likely to be opposed, or take a neutral stance, or say that they did not know.[198]

In all of this, it has to be stressed that the sample size of Muslim opinion was very small. Indeed, it was at the lowest level possible from which ICM would draw statistical conclusions. Even so, the results – given the often stark divergence from the population as a whole – can perhaps be seen as indicative of genuine trends, which appear to suggest a different outlook. Whether this is the product of a different set of cultural values, or merely a different interpretation of the questions at hand, can only be guessed at.

To conclude, what our survey of public attitudes demonstrates above all is the fact that there is a high level of public dissatisfaction with what is happening online regarding extremist content.

A clear majority of people feel that not enough is being done to prevent the spread of such content. Public opinion believes that the internet – and companies that inadequately police their platforms – require some form of regulation, preferably by an independent body, which will promote the deletion of extreme content. Moreover, the public are sufficiently convinced of the need for action in this sphere, and they are willing to see the curtailment of some liberties – at least online – in order to bring about change. Of course, that in itself does not justify the undermining of core freedoms, but it is perhaps indicative of the extent to which the Prime Minister was in tune with popular sentiment when she stated that the status quo was no longer tenable. In the battle against online extremism, there is a manifest feeling that it is time for change.

198 DS, 114-154.

Conclusion

The aim of this report was to understand the nature of the threat posed by online extremism – particularly as disseminated by the Sunni jihadist movement. This is the most pernicious and sustained form of extremist content currently being spread online, which poses a serious threat to the UK's national security and social peace.

Part one offered the most comprehensive analysis of the strategy and methodology of the online jihadist movement. It showed the consistency of output and the way that extremist content spreads from a core audience to a broader public, by means of a 'missionary' form of outreach. Attention was also drawn to the way in which extremist material is inadvertently being made more 'findable' by the actions of those who follow the jihadist movement for academic or journalistic purposes. Finally, an attempt was made to show why narratives that foreground a 'decline' of ISIS online are fundamentally misleading. The reality is that the jihadist movement continues to enjoy something of a virtual 'safe haven' and is enduring online, even as it is being rolled back in the real world.

In this context, part two considered a range of policy options for dealing with extremist content online. The impulse here was to look at this problem 'in the round', trying to tackle both ends of the food-chain: supply and demand. Emphasis was placed on the idea that society, as a whole, must take responsibility for tackling a number of different issues. Individual researchers must be careful that they do not, by their actions, unconsciously make it easier for extremist content to remain online. At the same time, it is clear that the mainstream internet companies can and should do far more to drive extremist content off their platforms. Recent months have seen a groundswell of pressure on this front. In the face of it, there are signs of movement, but too often the suspicion remains that the companies will do only the minimum necessary to head off the latest crisis of public confidence. As of yet, concrete action of a kind that would transform the situation remains elusive.

We recommend an approach based on the concept of 'responsive regulation', by which the government shows its readiness to implement a sliding scale of measures, that will bring pressure to bear on the companies to up their game. The aim here is not to antagonise those companies needlessly – the preference would be for a cooperative, mutually beneficial relationship; but the government must be prepared to act robustly to set the terms of trade, if it is to secure the best possible outcome.

Moreover, as this section of the report also proposes, the government should consider stronger action to try and limit the demand side of the extremism equation. One potential vehicle for this would be the creation of new legislative offences against the aggravated possession and persistent consumption of extremist material – modelled on the struggle against child pornography. Such legislation would send a powerful signal about the non-acceptability of such content, helping to set and enforce social norms. It could deter those drawn towards the path of radicalism and, simultaneously, prove a boon to overstretched security services. Doubtless, there are some who would look askance at any such proposal, but it is imperative that we ask tough questions and look for the most effective means to alter an unacceptable status quo. It is with this in mind that our proposals are deliberately provocative and aim to kickstart a debate around these issues.

The need for such a debate – and for fresh thinking – was made plain in part three, which examined public attitudes towards online extremism, as well as broader questions about liberty and security. What emerged is the fact that there is a clear popular appetite for change – and efforts to exert more online safeguards against the terrorist threat. It is evident that the public feels there is not enough being done to stop the spread of extremist material online. There is a clear perception that the internet companies are not living up to their responsibilities. A majority of people feel that the internet has become something akin to a virtual 'wild west'. Consequently, politicians are surely right to say – as have both the Prime Minister and Home Secretary – something must be done; that change is required; and the status quo is no longer acceptable.

If there is one message to emerge from all of this, it is surely that we – as a society – need to have a debate about the challenges posed by online extremism and the appropriate responses. It is vital that we arrive at something approaching a social consensus on fundamental questions:

- Where should the line be drawn when we seek to drive extremism out of the mainstream virtual space?
- How far should the State intervene to enforce certain moral and ethical norms of behaviour online?
- What are the responsibilities of the largest, most powerful corporations when it comes to policing the internet?

The hope is that this report can be a useful starting point for discussion on these and other issues. The policy responses outlined here offer one range of options for how society and government might proceed; undoubtedly, there are others. Whatever the solutions, it is clear that we, as a society, now need to ask difficult questions – to have, as has been said, uncomfortable and 'embarrassing conversations' – if we are to prevail in the struggle against online extremism.

Appendix 1

The full text of the relevant legislation is as follows:

Section 19 of the Public Order Act 1986

19 Publishing or distributing written material.

(1) A person who publishes or distributes written material which is threatening, abusive or insulting is guilty of an offence if—
(a)he intends thereby to stir up racial hatred, or
(b)having regard to all the circumstances racial hatred is likely to be stirred up thereby.
(2)In proceedings for an offence under this section it is a defence for an accused who is not shown to have intended to stir up racial hatred to prove that he was not aware of the content of the material and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting.
(3)References in this Part to the publication or distribution of written material are to its publication or distribution to the public or a section of the public.

The Racial and Religious Hatred 2006

[amends above Act to include]:

Acts intended to stir up religious hatred
29B Use of words or behaviour or display of written material
(1) A person who uses threatening words or behaviour, or displays any written material which is threatening, is guilty of an offence if he intends thereby to stir up religious hatred.
(2) An offence under this section may be committed in a public or a private place, except that no offence is committed where the words or behaviour are used, or the written material is displayed, by a person inside a dwelling and are not heard or seen except by other persons in that or another dwelling.
(3) A constable may arrest without warrant anyone he reasonably suspects is committing an offence under this section.
(4) In proceedings for an offence under this section it is a defence for the accused to prove that he was inside a dwelling and had no reason to believe that the words or behaviour used, or the written material displayed, would be heard or seen by a person outside that or any other dwelling.

(5) This section does not apply to words or behaviour used, or written material displayed, solely for the purpose of being included in a programme service.
29C Publishing or distributing written material
(1) A person who publishes or distributes written material which is threatening is guilty of an offence if he intends thereby to stir up religious hatred. Racial and Religious Hatred Act 2006 (c. 1) Schedule — Hatred against persons on religious grounds 4
(2) References in this Part to the publication or distribution of written material are to its publication or distribution to the public or a section of the public.
29D Public performance of play
(1) If a public performance of a play is given which involves the use of threatening words or behaviour, any person who presents or directs the performance is guilty of an offence if he intends thereby to stir up religious hatred.
(2) This section does not apply to a performance given solely or primarily for one or more of the following purposes— (a) rehearsal, (b) making a recording of the performance, or (c) enabling the performance to be included in a programme service; but if it is proved that the performance was attended by persons other than those directly connected with the giving of the performance or the doing in relation to it of the things mentioned in paragraph (b) or (c), the performance shall, unless the contrary is shown, be taken not to have been given solely or primarily for the purpose mentioned above.
(3) For the purposes of this section— (a) a person shall not be treated as presenting a performance of a play by reason only of his taking part in it as a performer, (b) a person taking part as a performer in a performance directed by another shall be treated as a person who directed the performance if without reasonable excuse he performs otherwise than in accordance with that person's direction, and (c) a person shall be taken to have directed a performance of a play given under his direction notwithstanding that he was not present during the performance; and a person shall not be treated as aiding or abetting the commission of an offence under this section by reason only of his taking part in a performance as a performer.
(4) In this section "play" and "public performance" have the same meaning as in the Theatres Act 1968.
(5) The following provisions of the Theatres Act 1968 apply in relation to an offence under this section as they apply to an offence under section 2 of that Act— section 9 (script as evidence of what was performed), section 10 (power to make copies of script), section 15 (powers of entry and inspection).
29E Distributing, showing or playing a recording
(1) A person who distributes, or shows or plays, a recording of visual images or sounds which are threatening is guilty of an offence if he intends thereby to stir up religious hatred. Racial and Religious Hatred Act 2006 (c. 1) Schedule — Hatred against persons on religious grounds 5

(2) In this Part "recording" means any record from which visual images or sounds may, by any means, be reproduced; and references to the distribution, showing or playing of a recording are to its distribution, showing or playing to the public or a section of the public.
(3) This section does not apply to the showing or playing of a recording solely for the purpose of enabling the recording to be included in a programme service. 29F Broadcasting or including programme in programme service (1) If a programme involving threatening visual images or sounds is included in a programme service, each of the persons mentioned in subsection (2) is guilty of an offence if he intends thereby to stir up religious hatred. (2) The persons are— (a) the person providing the programme service, (b) any person by whom the programme is produced or directed, and (c) any person by whom offending words or behaviour are used.
Inflammatory material
29G Possession of inflammatory material
(1) A person who has in his possession written material which is threatening, or a recording of visual images or sounds which are threatening, with a view to— (a) in the case of written material, its being displayed, published, distributed, or included in a programme service whether by himself or another, or (b) in the case of a recording, its being distributed, shown, played, or included in a programme service, whether by himself or another, is guilty of an offence if he intends religious hatred to be stirred up thereby.
(2) For this purpose regard shall be had to such display, publication, distribution, showing, playing, or inclusion in a programme service as he has, or it may be reasonably be inferred that he has, in view.

Section 57 of the Terrorism Act 2000

57 Possession for terrorist purposes.

(1)A person commits an offence if he possesses an article in circumstances which give rise to a reasonable suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism.
(2)It is a defence for a person charged with an offence under this section to prove that his possession of the article was not for a purpose connected with the commission, preparation or instigation of an act of terrorism.
(3)In proceedings for an offence under this section, if it is proved that an article—
(a)was on any premises at the same time as the accused, or
(b)was on premises of which the accused was the occupier or which he habitually used otherwise than as a member of the public,
the court may assume that the accused possessed the article, unless he proves that he did not know of its presence on the premises or that he had no control over it.
(4)A person guilty of an offence under this section shall be liable—

(a)on conviction on indictment, to imprisonment for a term not exceeding [15 years] , to a fine or to both, or
(b)on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.

Section 58 of the Terrorism Act 2000

58 Collection of information.

1) A person commits an offence if-
(a) he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or
(b) he possesses a document or record containing information of that kind.
(2) In this section "record" includes a photographic or electronic record.
(3) It is a defence for a person charged with an offence under this section to prove that he had a reasonable excuse for his action or possession.
(4) A person guilty of an offence under this section shall be liable-
(a) on conviction on indictment, to imprisonment for a term not exceeding 10 years, to a fine or to both, or
(b) on summary conviction, to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.
(...)

Section 1 of the Terrorism Act 2006

1 Encouragement of terrorism

(1)This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences.
(2)A person commits an offence if—
(a)he publishes a statement to which this section applies or causes another to publish such a statement; and
(b)at the time he publishes it or causes it to be published, he—
(i)intends members of the public to be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate acts of terrorism or Convention offences; or
(ii)is reckless as to whether members of the public will be directly or indirectly encouraged or otherwise induced by the statement to commit, prepare or instigate such acts or offences.
(3)For the purposes of this section, the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation of acts of terrorism or Convention offences include every statement which—
(a)glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences; and

(b)is a statement from which those members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.
(4)For the purposes of this section the questions how a statement is likely to be understood and what members of the public could reasonably be expected to infer from it must be determined having regard both—
(a)to the contents of the statement as a whole; and
(b)to the circumstances and manner of its publication.
(5)It is irrelevant for the purposes of subsections (1) to (3)—
(a)whether anything mentioned in those subsections relates to the commission, preparation or instigation of one or more particular acts of terrorism or Convention offences, of acts of terrorism or Convention offences of a particular description or of acts of terrorism or Convention offences generally; and,
(b)whether any person is in fact encouraged or induced by the statement to commit, prepare or instigate any such act or offence.
(6)In proceedings for an offence under this section against a person in whose case it is not proved that he intended the statement directly or indirectly to encourage or otherwise induce the commission, preparation or instigation of acts of terrorism or Convention offences, it is a defence for him to show—
(a)that the statement neither expressed his views nor had his endorsement (whether by virtue of section 3 or otherwise); and
(b)that it was clear, in all the circumstances of the statement's publication, that it did not express his views and (apart from the possibility of his having been given and failed to comply with a notice under subsection (3) of that section) did not have his endorsement.
(7)A person guilty of an offence under this section shall be liable—
(a)on conviction on indictment, to imprisonment for a term not exceeding 7 years or to a fine, or to both;
(b)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both;
(c)on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both.
(8)In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (7)(b) to 12 months is to be read as a reference to 6 months.

Section 2 of the Terrorism Act 2006

2 Dissemination of terrorist publications

(1)A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so—
(a)he intends an effect of his conduct to be a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism;
(b)he intends an effect of his conduct to be the provision of assistance in the commission or preparation of such acts; or
(c)he is reckless as to whether his conduct has an effect mentioned in paragraph (a) or (b).
(2)For the purposes of this section a person engages in conduct falling within this subsection if he—
(a)distributes or circulates a terrorist publication;
(b)gives, sells or lends such a publication;
(c)offers such a publication for sale or loan;
(d)provides a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan;
(e)transmits the contents of such a publication electronically; or
(f)has such a publication in his possession with a view to its becoming the subject of conduct falling within any of paragraphs (a) to (e).
(3)For the purposes of this section a publication is a terrorist publication, in relation to conduct falling within subsection (2), if matter contained in it is likely—
(a)to be understood, by some or all of the persons to whom it is or may become available as a consequence of that conduct, as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism; or
(b)to be useful in the commission or preparation of such acts and to be understood, by some or all of those persons, as contained in the publication, or made available to them, wholly or mainly for the purpose of being so useful to them.
(4)For the purposes of this section matter that is likely to be understood by a person as indirectly encouraging the commission or preparation of acts of terrorism includes any matter which—
(a)glorifies the commission or preparation (whether in the past, in the future or generally) of such acts; and
(b)is matter from which that person could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by him in existing circumstances.
(5)For the purposes of this section the question whether a publication is a terrorist publication in relation to particular conduct must be determined—
(a)as at the time of that conduct; and
(b)having regard both to the contents of the publication as a whole and to the circumstances in which that conduct occurs.
(6)In subsection (1) references to the effect of a person's conduct in relation to a terrorist publication include references to an effect of the

publication on one or more persons to whom it is or may become available as a consequence of that conduct.
(7)It is irrelevant for the purposes of this section whether anything mentioned in subsections (1) to (4) is in relation to the commission, preparation or instigation of one or more particular acts of terrorism, of acts of terrorism of a particular description or of acts of terrorism generally.
(8)For the purposes of this section it is also irrelevant, in relation to matter contained in any article whether any person—
(a)is in fact encouraged or induced by that matter to commit, prepare or instigate acts of terrorism; or
(b)in fact makes use of it in the commission or preparation of such acts.
(9)In proceedings for an offence under this section against a person in respect of conduct to which subsection (10) applies, it is a defence for him to show—
(a)that the matter by reference to which the publication in question was a terrorist publication neither expressed his views nor had his endorsement (whether by virtue of section 3 or otherwise); and
(b)that it was clear, in all the circumstances of the conduct, that that matter did not express his views and (apart from the possibility of his having been given and failed to comply with a notice under subsection (3) of that section) did not have his endorsement.
(10)This subsection applies to the conduct of a person to the extent that—
(a)the publication to which his conduct related contained matter by reference to which it was a terrorist publication by virtue of subsection (3)(a); and
(b)that person is not proved to have engaged in that conduct with the intention specified in subsection (1)(a).
(11)A person guilty of an offence under this section shall be liable—
(a)on conviction on indictment, to imprisonment for a term not exceeding 7 years or to a fine, or to both;
(b)on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum, or to both;
(c)on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or to both.
(12)In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003 (c. 44), the reference in subsection (11)(b) to 12 months is to be read as a reference to 6 months.
(13)In this section—
- "lend" includes let on hire, and "loan" is to be construed accordingly;
- "publication" means an article or record of any description that contains any of the following, or any combination of them—

(a) matter to be read;
(b) matter to be listened to;

(c) matter to be looked at or watched.

Section 3 of the Terrorism Act 2006

3 Application of ss. 1 and 2 to internet activity etc.

(1)This section applies for the purposes of sections 1 and 2 in relation to cases where—
(a)a statement is published or caused to be published in the course of, or in connection with, the provision or use of a service provided electronically; or
(b)conduct falling within section 2(2) was in the course of, or in connection with, the provision or use of such a service.
(2)The cases in which the statement, or the article or record to which the conduct relates, is to be regarded as having the endorsement of a person ("the relevant person") at any time include a case in which—
(a)a constable has given him a notice under subsection (3);
(b)that time falls more than 2 working days after the day on which the notice was given; and
(c)the relevant person has failed, without reasonable excuse, to comply with the notice.
(3)A notice under this subsection is a notice which—
(a)declares that, in the opinion of the constable giving it, the statement or the article or record is unlawfully terrorism-related;
(b)requires the relevant person to secure that the statement or the article or record, so far as it is so related, is not available to the public or is modified so as no longer to be so related;
(c)warns the relevant person that a failure to comply with the notice within 2 working days will result in the statement, or the article or record, being regarded as having his endorsement; and
(d)explains how, under subsection (4), he may become liable by virtue of the notice if the statement, or the article or record, becomes available to the public after he has complied with the notice.
(4)Where—
(a)a notice under subsection (3) has been given to the relevant person in respect of a statement, or an article or record, and he has complied with it, but
(b)he subsequently publishes or causes to be published a statement which is, or is for all practical purposes, the same or to the same effect as the statement to which the notice related, or to matter contained in the article or record to which it related, (a "repeat statement");
the requirements of subsection (2)(a) to (c) shall be regarded as satisfied in the case of the repeat statement in relation to the times of its subsequent publication by the relevant person.
(5)In proceedings against a person for an offence under section 1 or 2 the requirements of subsection (2)(a) to (c) are not, in his case, to be regarded as satisfied in relation to any time by virtue of subsection (4) if he shows that he—
(a)has, before that time, taken every step he reasonably could to prevent a repeat statement from becoming available to the public and to ascertain whether it does; and

(b)was, at that time, a person to whom subsection (6) applied.
(6)This subsection applies to a person at any time when he—
(a)is not aware of the publication of the repeat statement; or
(b)having become aware of its publication, has taken every step that he reasonably could to secure that it either ceased to be available to the public or was modified as mentioned in subsection (3)(b).
(7)For the purposes of this section a statement or an article or record is unlawfully terrorism-related if it constitutes, or if matter contained in the article or record constitutes—
(a)something that is likely to be understood, by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism or Convention offences; or
(b)information which—
(i)is likely to be useful to any one or more of those persons in the commission or preparation of such acts; and
(ii)is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.
(8)The reference in subsection (7) to something that is likely to be understood as an indirect encouragement to the commission or preparation of acts of terrorism or Convention offences includes anything which is likely to be understood as—
(a)the glorification of the commission or preparation (whether in the past, in the future or generally) of such acts or such offences; and
(b)a suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.
(9)In this section "working day" means any day other than—
(a)a Saturday or a Sunday;
(b)Christmas Day or Good Friday; or
(c)a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in any part of the United Kingdom.

Appendix 2

Convictions relating to the possession of extremist material (last three years):

2016

- **Abubakar Abubakar** was charged with possessing a document containing information of a kind likely to be of use to a person preparing or committing an act of terrorism contrary to section 58(1)(b) of the Terrorism Act 2000.
- **Zafreen Khadam** was charged with 10 offences of dissemination of terrorist publications contrary to section 2 of the Terrorism Act 2006. She was convicted after trial of all ten charges and received a 4 years' and 6 months' imprisonment. (Case is under appeal)
- **Mohammed Shaheryar Alam** was charged with disseminating a terrorist publication contrary to section 2 of the Terrorism Act 2006 on the basis that he was reckless as to whether it would encourage the commission or preparation of a terrorist act. He was convicted after trial and sentenced to two and a half years' imprisonment.
- **Mohammed Moshin Ameen** was charged with five offences of encouraging a terrorist act contrary to section 1 of the Terrorism Act 2006, one offence of disseminating a terrorist publication contrary to section 2 of the Terrorism Act 2006 and one offence of inviting support for a proscribed organisation contrary to section 12 of the Terrorism Act 2000. The judge noted that the offending was aggravated by the explicit and intentional nature of the encouragement and by the persistence with which it was pursued.
- **Ibrahim Anderson and Shah Jahan Khan** were charged with an offence of inviting support for a proscribed organisation contrary to section 12 of the Terrorism Act 2000. Mr Anderson was also charged with an offence contrary to section 58 of the Terrorism Act 2000 for possessing information of a kind likely to be of use to someone intending to carry out an act or acts of terrorism.
- **Naseer Taj** was charged with one offence contrary to section 5 of the Terrorism Act 2006 and two offences contrary to Section 58 of the Terrorism Act 2000 and an offence contrary to section 4 of the Identity Documents Act 2010.

- **Rebecca Poole** was charged with one offence of collecting information likely to be useful to a person committing or preparing an act of terrorism, contrary to section 58 of the Terrorism Act 2000. The court found her found not fit to plead but to have been in possession of the material. She was made subject to a Hospital Order with restrictions.
- **Abdul Hamid** pleaded guilty to dissemination of a terrorist publication, contrary to section 2 of the 2006 Act and was sentenced to two years' Imprisonment with 10 years' Terrorism Notification Order.

2015

- **Hassan Munir** pleaded guilty to an offence of disseminating a terrorist publication contrary to section 2 Terrorism Act 2006.
- **Usman Choudhary** pleaded guilty to one offence of disseminating a terrorist publication, contrary to section 2 of the Terrorism Act 2006, for sending the book into the prison and was sentenced to 9 months' imprisonment.
- **Alaa Esayed** pleaded guilty to an offence contrary to section 1 of the Terrorism Act 2006 and an offence contrary to section 2 of the Terrorism Act 2006.
- **Ednane Mahmood** was charged – and subsequently convicted – with offences contrary to section 5 of the Terrorism Act 2006 (preparation of terrorist acts) and section 2 of the Terrorism Act 2006 (dissemination of terrorist material).
- **Mustafa Abdullah** was convicted of 13 offences contrary to section 58 of the Terrorism Act 2000.
- **Atiq Ahmed** was charged with two offences of disseminating a terrorist publication contrary to section 2 Terrorism Act 2006. On 6 August 2015, he pleaded guilty.
- **Malcolm Hodges** was charged with one offence of encouraging terrorism contrary to section 1 of the Terrorism Act 2006 and one offence of possession of a document of a kind likely to be useful to a person committing or preparing an act of terrorism contrary to section 58 of the Terrorism Act 2000. He pleaded guilty.
- **Y** is a 16-year-old girl (and therefore cannot be named) who pleaded guilty to two offences of possessing information of a kind likely to be useful to a terrorist contrary to section 58 of the Terrorism Act 2000.
- **Abdul Miah** was charged with two offences of disseminating terrorist publications, contrary to section 2 of the Terrorism Act 2006. He is an ISIS follower who used the internet to disseminate films that encouraged terrorism through violence including martyrdom.
- **Adeel Amjad** was charged with one offence of possessing a document containing information of a kind likely to be useful to a person

committing or preparing an act of terrorism contrary to section 58 of the Terrorism Act 2000.

- **Mohammed Kahar** was convicted on multiple separate counts (preparation for terrorist acts, funding, inviting support, *and dissemination*).

2014

- **Ibrahim Hassan and Shah Hussain**, pleaded guilty to jointly disseminating an Anwar al-Awlaki video on their You Tube channel.
- **Mohammed Saeed Ahmed and Mohammed Naeem Ahmed** pleaded guilty to a number of offences contrary to section 58 of the Terrorism Act 2000, in that they collected or made a record of information that was of a kind likely to be useful to a person committing or preparing an act of terrorism by causing or permitting to be created on a variety of electronic devices over a number of dates.
- **Runa Khan** pleaded guilty to disseminating a terrorist publication contrary to section 2(1) and 2 (e) of the Terrorism Act 2006.
- **Andrea Pierides**, was charged with possessing information likely to be useful to a person committing or preparing an act of terrorism to contrary to Section 58(1)(b) of the Terrorism Act 2000.
- **Ryan McGee** was charged with possession of a document (The Anarchist's Cook Book) for terrorist purposes, contrary to section 58 of the Terrorism Act 2000 and making an improvised explosive device (IED), namely a 'nail bomb' contrary to section 4 Explosive Substances Act 1883.
- **Afsor Ali** was charged and convicted of possession of documents or records containing information of a kind likely to be useful to a person committing or preparing an act of terrorism contrary to Section 58 of the Terrorism Act 2000.

Appendix 3

Draft Sentencing Guidelines:
Possession and/or Consumption of Extremist Material

Law to prohibit 'the 'aggravated possession and/or persistent consumption of material that promotes hatred and/or violence, in the service of a political ideology'.

Triable only on indictment
Maximum: 7 years imprisonment

Offence range: warning – 7 years

This guideline applies only to offenders aged 18 and older

STEP ONE **Determining the offence category**	
The court should determine the offence category with reference **only** to the factors listed in the tables below. In order to determine the category, the court should assess **culpability** and **harm.** The court should weigh all the factors set out below in determining the offender's culpability. **Where there are characteristics present which fall under different levels of culpability, the court should balance these characteristics to reach a fair assessment of the offender's culpability.**	
Culpability demonstrated by one or more of the following:	
A	• Possession of significant number of articles that constitute extremist material explicitly promoting hatred/or violence of the most pernicious kind • Repeatedly consumed (viewed/read/listened) to such material • Consumption or possession was conscious and enthusiastic • Consumption or possession with a view to dissemination/promotion
B	• Cases falling between A and C
C	• Possession of articles that constitute extremist material but of a less pernicious kind and in smaller volume • Repeated consumption of such material but more ad hoc and not as part of determined engagement with such material • Consumption or viewing was not driven by any wider practical purpose

Harm The court should consider the factors set out below to determine the level of harm that has been **caused or risked.**	
Category 1	• Articles include the most extreme forms of violence, including murder, torture, sadism (beheading etc.)
Category 2	• Articles that explicitly encourage a resort to violence (for example, calls to physical force/violent jihad) • Articles that explicitly promotes sectarian hatred (e.g. explicit forms of takfiri pronouncement) the articulation of virulent anti-semitism or the denigration of other faiths ("Hindus are excrement" etc.)
Category 3	• Articles that promote hatred against women and racial, religious or sexual minorities • Articles that implicitly promotes a resort to violence

STEP TWO **Starting point and category range**
Having determined the category at step one, the court should use the corresponding starting point to reach a sentence within the category range below. The starting point applies to all offenders irrespective of plea or previous convictions. A case of particular gravity, reflected by multiple features of culpability or harm in step one, could merit upward adjustment from the starting point before further adjustment for aggravating or mitigating features, set out on the next page.

Harm	Culpability		
	A	B	C
Category 1	**Starting point** 6 years' custody **Category range** 5-7 years' custody	**Starting point** 4 years' custody **Category range** 3-5 years' custody	**Starting point** 2 years' custody **Category range** 1-3 years' custody
Category 2	**Starting point** 2 years' custody **Category range** 1-3 years' custody	**Starting point** 1 year custody **Category range** 26 weeks-2 years' custody	**Starting point** 26 weeks' custody **Category range** 13-52 weeks' custody
Category 3	**Starting point** 26 weeks' custody **Category range** 13- 52 weeks' custody	**Starting point** 13 weeks' custody **Category range** Asbo - 26 weeks' custody	**Starting point** Formal warning plus mandatory referral to Prevent **Category range** Formal warning plus mandatory referral to Prevent-Asbo

Below is a **non-exhaustive** list of additional factual elements providing the context of the offence and factors relating to the offender. Identify whether any combination of these, or other relevant factors, should result in an upward or downward adjustment from the sentence arrived at so far. In particular, relevant recent convictions are likely to result in an upward adjustment. In some cases, having considered these factors, it may be appropriate to move outside the identified category range.

Factors increasing seriousness
Statutory aggravating factors:

- Previous convictions, having regard to a) the **nature** of the offence to which the conviction relates and its **relevance** to the current offence; and b) the **time** that has elapsed since the conviction
- Offence committed whilst on bail
- Volume of material in question
- Individual involved in a network that encouraged the consumption of such material
- ***Other aggravating factors:***
- Failure to respond to warnings against consumption/possession of material
- **Factors reducing seriousness or reflecting personal mitigation**
- No previous convictions **or** no relevant/recent convictions
- Good character and/or exemplary conduct
- Evidence of a change of mind set prior to arrest
- Mental disorder or learning disability, particularly where linked to the commission of the offence

STEP THREE
Consider any factors which indicate a reduction for assistance to the prosecution
The court should take into account sections 73 and 74 of the Serious Organised Crime and Police Act 2005 (assistance by defendants: reduction or review of sentence) and any other rule of law by virtue of which an offender may receive a discounted sentence in consequence of assistance given (or offered) to the prosecutor or investigator.

STEP FOUR
Reduction for guilty pleas
The court should take account of any potential reduction for a guilty plea in accordance with section 144 of the Criminal Justice Act 2003 and the *Guilty Plea* guideline.

STEP FIVE
Dangerousness
The court should consider whether having regard to the criteria contained in Chapter 5 of Part 12 of the Criminal Justice Act 2003 it would be appropriate to impose an extended sentence (section 226A).

STEP SIX
Totality principle
If sentencing an offender for more than one offence, or where the offender is already serving a sentence, consider whether the total sentence is just and proportionate to the overall offending behaviour in accordance with the Offences Taken into Consideration and Totality guideline.

STEP SEVEN
Ancillary orders
In all cases the court should consider whether to make ancillary orders.

STEP EIGHT

Reasons
Section 174 of the Criminal Justice Act 2003 imposes a duty to give reasons for, and explain the effect of, the sentence.

STEP NINE
Consideration for time spent on bail
The court must consider whether to give credit for time spent on bail in accordance with section 240A of the Criminal Justice Act 2003.

Policy Exchange

In this major new report, Policy Exchange provides a comprehensive analysis of the struggle against online extremism – the 'new Netwar'. The spate of terrorist attacks in the first half of 2017 confirmed that jihadist radicalisation is a real and present danger to the national security of the UK and its allies. Yet talk of ISIS' 'decline' in the virtual world has been grossly overstated. The group has shown itself to be adaptable and durable – in spite of the loss of its physical strongholds – and there is a danger that the blood and treasure we have invested in Iraq and Syria will produce little more than a pyrrhic victory. ISIS is producing extremist content online at a consistent rate and this is spread across a vast information ecosystem: it is disseminated to core followers via Telegram, before being pumped out into the mainstream social media space (via Twitter, Facebook and other leading platforms). For this reason, we argue that more must be done to force jihadist content out of the mainstream. It is clear that the status quo is not working; it is time for a new approach.

Our major survey of public opinion shows that two-thirds of people believe the leading social media companies are not doing enough to combat online radicalisation. Three-quarters of people want the companies to do more to locate and remove extremist content. In this report we explore a range of policy options for interdicting the supply-chain of extremist content - at both ends. We urge the government to pursue a tougher line with the mainstream companies - to force them to clean up their act. Equally, we suggest the government may wish to consider new legislation to counter the possession and consumption of extremist material online. Through these and other measures, we argue that society as a whole must act to overcome this serious threat to the security, vitality and prosperity of western societies.

ISBN: 978-1-910812-34-1

Policy Exchange
8 - 10 Great George Street
Westminster
London
SW1P 3AE

www.policyexchange.org.uk