Centre on Religion & Geopolitics

digitālis REPUTATION

A WAR OF KEYWORDS

How extremists are exploiting the internet and what to do about it

Mubaraz Ahmed

Fred Lloyd George

The Centre on Religion & Geopolitics is part of the Tony Blair Faith Foundation which is registered with the Charity Commission of England and Wales with the number 1123243. We are a company limited by guarantee and registered in England and Wales with company number 06198959. Our registered office is 66 Lincoln's Inn Fields, London, WC2A 3LH. The Tony Blair Faith Foundation US has been determined by the IRS to be a publicly-supported 501 (c) 3 organisation which can receive tax-deductible contributions from US donors. As an independent US tax-exempt organisation, TBFF US shares the goals of, and provides support to, the Tony Blair Faith Foundation based in London.

A WAR OF KEYWORDS

How extremists are exploiting the internet and what to do about it

Mubaraz Ahmed

Fred Lloyd George

TABLE *of* CONTENTS

Foreword

Twenty years ago I was running my first internet marketing business, evangelising new technology and urging corporate participation. Most of my counsel today, whether to schools, business, or government, instead involves advising a cautionary pause and consideration of physical security, cyber and reputational risk. This digital era has brought about profound positive change, but at such a pace that its risks are often not immediately apparent.

During that time, of course, the role of the internet has grown beyond information, marketing, and research to dominate increasingly shopping, entertainment, and new but ubiquitous forms of social interaction. The majority have spent the last 10+ years documenting their lives online (creating a treasure trove of data for marketers, but also for those with malintent) and most use apps and social media daily. With so many online channels and new specialisms, the challenge of knowing one's audience and how they behave is tougher than ever. In this respect, the role of the marketer and of the radical preacher is analogous.

Consumer marketers learnt many new disciplines fast, but as recently as this year, the leader of a political party proudly showed me his website and Facebook page as evidence of a "digital strategy." I told him that his "build it and they will come" website reaped few visitors and that those constituents who befriended him on Facebook were already his fans anyway. He didn't seem to know what they were doing about targeting those whom they sought to convert and with whom they so desperately needed to engage.

With so much reporting on how extremists use social media to spread their propaganda, one might be forgiven for believing that this is the new front line in the battle. Funnily enough I don't follow any radical preachers on social media so – just like the innocent teenager whom they target for recruitment – I don't tend to happen upon their hate speech therein.

While the true devotee of any cause may be linked through social channels to their idols, early innocent research – often by the most vulnerable – plays out in a different battlefield, which is still dominated by search engines.

A sophisticated recruiter (marketer and groomer alike) recognises his or her target audience's behaviour; attracting them at this early point with non-radical but enticing bait in search engines; exposing targets later to increasingly radicalised content, and pinpointing those with whom that content will best resonate.

The tech giants are the de facto scapegoat and it is easy for the layman to assume they have the power to "switch off" dark content. My view is that there are real limitations to their abilities to act. Facebook, for example, was criticised because Fusilier Lee Rigby's killer had earlier mooted on Facebook his intent to "kill." Facebook boasts over one-and-a-half billion users who create five billion Likes per day and, while the company's advertising model is based on automatically mining the content its users create, their ability to distinguish a single credible "kill" threat from the plethora who have threatened to "kill" in jest is highly limited.

In fact, when given credible options to play their part, Facebook, Google et al appear to be committed and collaborative in their investments in combatting extreme content. But they do not boast the ability to pinpoint the extremist or to detect the often nuanced narrative. In that challenge, the minds and machines of others are needed.

Digitalis boasts technology used by businesses to displace legacy issues from, or to balance debate within, search engine listings; the Centre on Religion & Geopolitics (CRG) has acclaimed expertise in global extremism, radicalisation, and ideology. These teams worked together based on my hypothesis that the same principles and technology we use to rebalance debate online might be used to better promote counter-narratives to extremist messages; certainly to counterbalance, but potentially to outrank its radical opponent in search engines.

The resultant research and analysis distilled an exhaustive internet trawl into meaningful – and ground-breaking – insights. This study's findings, if acted upon by governmental and non-governmental stakeholders, will have a meaningful impact on the path of the most vulnerable online, removing one tool in the armoury of the modern day extremist.

Dave King, CEO Digitalis

Executive Summary

When Donald Trump suggested he would build a wall on the Mexican border, Hillary Clinton retorted, "How high does a wall need to be to keep out the internet?" Today, radicalisation takes place in bedrooms, in libraries, on mobile phones. Connectivity and globalisation cannot be stopped – nor should they. But how can we stop the oncoming traffic of internet radicalisation?

The emergence of ISIS and its use of the internet for recruitment and propaganda has been a stark reminder of how the web can be a platform for dangerous ideas. Time and again, we have seen how radical thinking online has violently manifested itself in the offline world.

To grasp the scale of this challenge, and to be adequately placed to combat it, we need to diagnose the extent of Islamist extremist material on the internet.

AIM

Research into online radicalisation has mainly focused on two areas of enquiry: the role of social media and ISIS' activity online. But there is much more to the internet than social media. This study will endeavour to shed light on how accessible extremist content is outside of social media, with a particular focus on the role played by the search engine Google. Initiatives for better understanding extremism on the internet have predominantly been led by experts in extremist ideology or the sociological aspects of radicalisation. Technology firms, key stakeholders in this fight, have played a less prominent role.

This study set out to look beyond the usual suspects of Facebook, Twitter, and Telegram. We wanted to gain a greater understanding of the broader reach of extremist ideology online. This focus on social media and bots,[1] the deep and dark web, and how ISIS is harnessing these, has dominated the conversation. Not enough attention has been paid to the wider online landscape, where a broad array of extremist material has flourished, unchallenged.

In a similar vein, recent attention on online extremism has focused on violent material and a handful of groups. But there is an entire spectrum of content online, which expresses ideas that undermine the rule of law and spreads intolerant attitudes. This includes non-violent Islamist groups who call for the downfall of democratic systems and the introduction of a caliphate. It also includes Salafi websites that insist on death for apostates.

ISIS may seem like the apex of Islamist extremism, but it shares an ideology with a number of groups and individuals who seek the same objectives and share a worldview. The Centre on Religion & Geopolitics (CRG) and Digitalis set out not only to identify jihadi content online, but also the extent to which non-jihadi extremist content is accessible to users online. Specifically, we wanted to find out how easily the average user could access extremist material.

The debate around how best to combat extremist content online almost inevitably raises questions about the threat posed to civil liberties. While the removal of child pornography or graphic violence is widely agreed upon by governments and technology companies, efforts to counter online extremism should not be used to curb individual rights. Counter efforts must adopt a proactive approach and seek to drown out extremist content, rather than focusing solely on removing it.

OVERVIEW

This research centred on three layers of analysis: Firstly, understanding the keywords, or search terms, people use to find information on Google; secondly, looking at the data demonstrating links going into a selection of known extremist websites in order to understand their relationships with other websites;[2] and thirdly, analysing the content of Google search results pages to understand the placement

[1] A bot is a software application that runs automated tasks, or scripts, often over the internet. The use of bots in the distribution of extremist content has previously been researched. See J.M. Berger and Jonathon Morgan, *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*, Brookings, Washington DC: March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

[2] Linking data identifies all the variant websites that link, and therefore facilitate access into, a particular website.

of extremist and counter-narrative content within search results for relevant keywords. The areas of analysis represent important aspects related to the broader internet and, when combined, gave the opportunity to get a snapshot of extremist content beyond the realm of social media.

The results produced by this multi-faceted approach provide an overview of extremist content online and shed much-needed light on the impact and effectiveness of online counter-narrative efforts.

As part of the study, we looked at:

- The average monthly number of global searches conducted in Google (search frequencies) for **287** extremism-related keywords, **143** in English and **144** in Arabic.
- Regional search frequencies in **33** regions, including **six** US cities, **eight** UK cities, and **11** countries from the Middle East and North Africa.
- The first two search engine results pages for **47** keywords to determine rankings of extremist and counter-narrative content, looking at a total of **870** web pages.
- The linking data of **45** websites containing extremist content, in order to understand inter-website relationships and search engine optimisation (SEO) efforts.

KEY FINDINGS

1 A Wide Range of Extremist Content is Available Online

This study found a broad array of extremist content on websites, including violent and non-violent publications. Extremist views on sectarianism, apostasy, and conspiratorial attitudes towards the West – ideas that permeate much of ISIS' output – feature on widely used, mainstream Islamic websites. We found that, of the extremist content accessible through these specific keyword searches, **44 per cent was violent, 36 per cent was non-violent, and 20 per cent was political Islamist content**, i.e. non-violent content propagated by, or in support of, a known Islamist group with political ambitions.

2 Web Searches are a Gateway to Violent Extremist Content

The average, interested internet user requires nothing more than a simple Google search to gain access to extremist publications from groups like ISIS and al-Qaeda. Whether through analysis sites or otherwise, jihadi content is accessible via Google, without the need for social media. From our sample, we found that there are on average in the region of **more than 484,000 Google searches globally, and at least 54,000 searches in the UK alone, each month for keywords that return results dominated by extremist material.** While a wide range of people may have conducted some of these searches, including journalists, researchers, and students, the risk posed by the prevalence of extremist content in the results for these keywords remains a concern.

3 High-Risk Keywords Go Unchallenged by Counter-Narratives

Despite the emergence of online counter-narrative initiatives in recent years, these narratives are desperately weak in their presence in search engine results pages (SERPs). They do not sufficiently contest or dominate extremist ideas online. After analysing the SERPs for 47 relevant keywords, we found that **counter-narrative content outperformed extremist material in only 11 per cent of the results generated.** The SERP analysis in this study showed that the content returned for popular keywords often associated with extremism online, such as 'ISIS,' 'Islamic State,' and 'jihad' in fact pose no threat at all. However, extremist content that appears in searches for words that have appeared in discourse in recent years such as 'caliphate' and 'Dabiq' – the name of ISIS' English-language magazine – goes unchallenged. Efforts to counter extremism online are lagging behind in agility and diversity.

4 Mainstream Islamic Websites are Hosting Extremist Content

Through the analysis of SERPs and website links it became evident that **a number of sites purporting to present legitimate Islamic scholarship also host extremist material.** This is true of forums, 'Q&A' websites, and online repositories that contain books and lectures by known jihadis such as Anwar al-Awlaki, a US-born jihadi ideologue for al-Qaeda in the Arabian Peninsula (AQAP), and Abdullah Azzam, an early al-Qaeda ideologue and chief controller of the Arab-Afghan Mujahedeen movement. This material is available without any warning or safeguards in place. In some cases, when users were directed to sites for Islamic content, such as translations of the Quran or books of Hadith literature,[3] they were in fact entering sites hosting politicised Islamist and jihadi content. Users who trust a site's legitimate Islamic content may become vulnerable to extremist ideas they encounter on that same site.

5 Non-Violent Islamists Have a Strong Online Presence

Hizb ut-Tahrir, a global pan-Islamic movement that seeks to establish an Islamic state, has a very strong online presence and dominates the results for a number of the keyword searches in our sample. The group operates a series of websites, including its central site and regional affiliate websites that support Hizb ut-Tahrir's global aims. Furthermore, our

[3] Hadith literature refers to the collection of the reported actions and sayings of the Prophet Mohammad.

research showed that **political Islamist content by Hizb ut-Tahrir, its affiliates, and its supporters accounted for 20 per cent of all the extremist content identified**.

6 Counter-Narratives are Lagging, but Muslim Efforts Dominate

Counter-narrative efforts appear in only 43 of the 870 results analysed, just five per cent of the total, demonstrating their failure to challenge the extremist content found in the the SERPs. Linking data from established counter-narrative sites showed that these initiatives lack SEO efforts. Counter-narrative websites were also found to not rank high enough in searches to challenge extremist content. Of the counter-narratives identified, 91 per cent were Muslim-led efforts. This highlights the efforts being taken by Muslims to address the rising tide of extremist ideologies online.

It is estimated that close to three billion people have access to the internet around the globe, a number expected to swell to more than seven billion by 2020.[4] The need to address extremism online and safeguard internet users has never been more pressing.

This report provides a brief, albeit targeted, reflection of a tiny slice of the constantly growing and evolving world wide web, and access to extremist content on it. More importantly, our research is designed to inform governments, technology companies, and civil society groups fighting online extremism about how accessible and prolific this material is online.

This ever-evolving landscape, accessed by almost half of the world's population, must be secured in order to prevent extremism online from manifesting offline. We need a cohesive, integrated, and concerted effort to root out extremist ideologies on the internet. But we will only succeed if all those involved fully understand the scale and implications of this unprecedented problem.

[4] The Broadband Commission, *The State of Broadband 2014: Broadband for All*, Geneva: September 2014, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2014.pdf.

Policy Recommendations

A GLOBAL COMMITMENT ON SAFEGUARDING THE INTERNET

In the modern age, where internet access is considered a right rather than a privilege, an integral part of global connectivity, more must be done to unite the disparate actors working to make the internet safer. For these efforts to succeed, there is a pressing need for a comprehensive and multi-faceted commitment to securing the online landscape.

Existing agreements in this area have either been limited to specific countries or regions, or have only included a handful of major technology companies. For any such effort to be effective, it will require international cooperation from governments, the private sector, and the third sector.

The internet transcends borders. It is used by people from all religious, economic, educational, and social backgrounds. Keeping this vast realm open and secure requires cooperation from as many countries as possible, from multi-million dollar technology corporations to start-ups, from civil society groups, religious organisations, and communities.

Governments, technology companies, civil society groups, and religious organisations should:

- Establish a charter setting out the efforts needed to win the online battle, with a broad spectrum of actors signing up and pledging to make the internet a safer place for everyone.
- Come together in agreement, not only on collectively accepting a full-spectrum definition of extremism online, but also pledging to contribute to the global effort to eradicate it through initiatives in formal and informal educational programmes.

COOPERATION AND INTEGRATION IS KEY TO SUCCESS

Our research shows that extremist content continues to be readily accessible to the average user, and that a successful response is urgent. Only by joining forces will it be possible to address toxic ideas that exist in the online landscape unchallenged. Governments, civil society, and technology companies all have a role to play in this battle. There is a need to pool together the resources and expertise from all these actors. They all have a stake in this fight.

Governments should:

- Establish a global taskforce under the auspices of the UN focusing on countering online extremism, with the aim of calling on experts from a full spectrum of technology services, research units focused on extremism, and religious groups in order to better understand the diversity of extremist material on the internet and modes of transmission. This would help better inform counter efforts.

Governments, civil society, and technology companies should:

- Pool resources in order to fight the online battle of ideas together. This will help harness the entrepreneurial spirit of the technology field. Establishing a central command centre for tackling extremism online will help better coordinate expertise, materials, and funding to ensure there is a coherent and well-supported effort to tackle this issue. The command centre would also coordinate tasks across the relevant partners to ensure clarity and maximise effect and efficiency.
- Facilitate greater interaction between all three fields through events to share subject knowledge and build effective policy measures. For example, working together to organise conferences, workshops, and briefings in order to foster greater cooperation in counter-extremism efforts.

Technology companies should:

- Open channels of communication in order to provide a greater level of access to government and civil society. This includes providing practical support on improving search engine optimisation (SEO) and bolstering online presence in order to inform government and civil society strategies to shift the balance in the online space, as well as sharing analytical data and trending information to bolster counter efforts.

Civil society should:

- Reach out to a full spectrum of technology services and companies to collaborate with in tackling extremism online. While major internet firms like Google, Facebook, Twitter, and Microsoft are often the first point of call for such efforts, there are many others that can also bring added value to the fight. Many internet companies, small or large, have much-needed expertise to offer in the battle to safeguard the online landscape.

CREATE STRONG COUNTER-NARRATIVES THAT COMPETE IN THE CORRECT SPACES

We need strong counter-narratives that are relevant to the correct audience, ideologically and visually, and that are targeted at keywords that currently lack balance in search results. Analysis of the search engine results pages (SERPs) and the content returned showed that of all the counter-narrative efforts identified, 91 per cent were Muslim-led. Government-led efforts were mostly absent in the searches. Efforts should be made to harness the power of Muslim voices already working to counter extremist ideologies. We should ensure they have the resources to do so successfully.

Governments should:

- Support rather than front counter-narratives online. Governments should ensure that funding, technical expertise, and all other necessary resources are available to Muslim groups seeking to introduce more moderate voices online. Our research suggests that government-fronted counter-narratives do not receive enough attention to feature prominently in search results. Alternatively, governments can support the creation of content that engages with a given topic, through guidance and sponsorship of third parties.

- Understand the potential of other technological firms and services beyond major corporations. There is a wide community of technology companies that have developed tools that could support the promotion of counter-narratives. A range of companies possess the technological expertise and experience to redress the balance online. They can collaborate with others working to counter extremism on the web.

Civil society should:

- Monitor and evaluate the success and failures of existing counter-narrative initiatives by working more closely with technology companies who have the tools to help understand how counter-narratives are performing online. Our research suggests that counter-narratives are poorly positioned on the web and do not reach the right audiences.

- Research online behaviours of target audiences. Experts have called on counter-narratives to match the propaganda produced by ISIS and al-Qaeda. But our research shows that the strongest, most prominent websites within the search engine results expressing extremist ideas are not necessarily those with expensive or professional videos. The simplicity of many of these sites shows you do not need a sophisticated platform to attract attention.

Technology companies should:

- Alter operating procedures in order to support the introduction of the counter-narrative voice. Search engine companies have been demonstrably reluctant or unable to alter their search algorithms, which are responsible for search page rankings, however a change of tack may help facilitate the introduction of counter-narrative efforts. By doing so, search companies can ensure that counter-narrative efforts feature prominently in the organic search results and are well-placed to challenge extremist ideas online.

- Promote counter-narrative content in organic areas (anything that is not paid content) online using expertise in the field. In the short term, paid advertising may be a suitable option for promoting counter-narratives, but it is not a sustainable solution. Further, it will not address weighting towards extremist content for crucial keywords on the SERPs.

A FULLER UNDERSTANDING OF EXTREMISM ONLINE IS NEEDED

We need to move beyond the focus on ISIS and al-Qaeda propaganda online, and to acknowledge the presence of extremist ideas around the web. Making the distinction between violent and non-violent extremism is important when taking action against groups offline, but online the differences are far murkier, and they are less pronounced. Our research found that non-violent Islamist extremist content has a strong online presence, and much of this material overlaps with ideas presented in ISIS and al-Qaeda propaganda. A focus on explicitly violent material, or on content produced by a handful of extremist groups, ignores the plethora of potentially radicalising content elsewhere on the internet, which is accessible through simple online searches. Even mainstream, moderate websites have been shown to host jihadi content, making it harder to distinguish between moderate Islamic content and extremist content.

Governments should:

- Work to broaden current classifications on what is deemed extremist content online to incorporate non-violent extremist content. Just as there are clear definitions of copyrighted material, child pornography, and hate speech, all of which have been subject to removal requests, there must be an agreed upon definition of extremist content in order to properly guide and inform online efforts against it.

- There must be greater consistency in the application of the law. Anti-terror legislation in a number of countries has been used to pursue individuals in possession of extremist material or who express particular views. Yet, the same crimes generally go unpunished online.

Governments and civil society should:

- Build online literacy for users by introducing workshops into schools that teach skills to help navigate the internet and apply critical thinking to sources found on the web.

- Explore the potential of working with filtering companies to monitor online trends surrounding extremism. Existing content-control software that prevent access to graphic or age-restricted content could be used to block access to extremist material. Specialist technology companies have developed advanced and precise online monitoring devices. Using pooled resources from government, internet providers, and the large technology firms, these companies could be outsourced to monitor known keyword results pages that pose a threat to users and identify new trends online.

Technology companies should:

- Outsource content control to third-party, subject-matter experts in order to effectively understand and address the wide variety of extremist content online. This support would alleviate the current burden on large technology companies to conduct content control. It would also allow experts to make judgements on what constitutes extremist content and where it is likely to appear in the wider web, and it would allow governments to support online counter-extremism work.

- Ensure users are made aware through warning messages that they may be entering a site with extremist material. This is particularly important for those sites that have been identified in this research as hosting extremist content that is not necessarily violent, or which sits alongside non-extremist material. Much like existing age restrictions for websites with adult content, pre-warnings for extremist content could prevent users unintentionally accessing potentially radicalising material.

PROVIDE ACCESS TO ANSWERS IN OFFLINE AND ONLINE ENVIRONMENTS

Our research confirms that forums and 'Q&A' websites are very popular among users seeking information about Islam. This tells us how people are drawn online when looking for answers and advice on specific topics.

Governments and civil society should:

- Provide offline opportunities for people to take part in interactive dialogues around common questions users are asking online. Such opportunities could be provided through workshops, 'Q&A' forums, and greater access to credible, moderate Muslim voices in schools and universities, religious institutions, and community groups.

- Establish online spaces that offer a safe and moderated environment for individuals to ask questions. This could be done by following existing formats such as 'Q&A' sites, forums, or by pursuing alternative methods such as online chat 'helpdesks' or video chat platforms.

PART ONE

Introduction

When Aqsa Mahmood left her home in Glasgow in 2013 to join ISIS, her family was sure the 21-year-old had been radicalised online. Described by those who knew her as "sweet," "peaceful," "intelligent," and "well integrated," the family's lawyer, Aamer Anwar urged: "If this could happen to someone like her, someone so intelligent, then it could happen to anybody."

Aqsa, a 'bedroom radical,' is thought to have been influenced by sermons and teachings she accessed online. Her story, though not unique, highlighted the role that extremist material on the internet plays in radicalising individuals.

Whether on computers, tablets, or mobile phones, we know that extremist material is available on the web, and that the internet is a major facilitator of radicalisation today. According to UK policy documents and senior investigating police officers, the internet is often a mobilising factor in terrorism cases. It is increasingly rare for the world wide web to play no role at all.[5] Research confirms this: In a study of 15 cases of extremism and terrorism in the UK, all the suspects had been radicalised in part by online content.[6]

And yet, the nature and scale of the problem are gravely misunderstood. How easily can an individual access extremist material? Where is this content hosted? And to what extent are potentially radicalising websites being challenged online with counter-narratives?

Aqsa Mahmood's online behaviour was not unusual. She is one of millions who spend hours a day on the internet. For so many of her generation, worldviews are shaped largely in the virtual world. Search engines have overtaken libraries and classrooms as sources of information. Websites like Google are the first port of call in our quest for knowledge and understanding.

Studies and commentary often focus on social media as a tool for dispersing extremist content and for jihadi recruitment. But social media does not tell the whole story; it is just one online arena that extremists use. To access extremist content via social media, you need to know where to look. In most cases, individuals will already have been exposed to extremist thinking through social circles offline, or they will be aware of accounts disseminating content and will actively follow them on Twitter, Facebook, and other platforms. Social media tends to connect likeminded individuals, rather than being the method of radicalisation itself. At the stage where someone has followed a hashtag or joined a group, they have likely already been convinced by an ideology, or at the very least been open to its ideas. What is more, when looking for information, the vast majority of online users start via search engines, not social media. Research suggests that 90 per cent of people use search engines to navigate the internet, with 82 per cent of users opting for Google.[7] Despite these figures, discussions of online extremism refer almost exclusively to social media as the major facilitator. While the role of social media in radicalising individuals has been documented, an overt focus on social media platforms has created a blind spot when it comes to the wider web.

This study looks at that blind spot. As such, like the vast majority of internet users, this study centres around the Google search engine. The keywords typed into Google play a vital role online; analysing search frequencies for a selection of keywords gives insight into how people access extremist content. To begin to understand how users might come into contact with radicalising online material, we analysed the search frequencies of 147 English keywords related to violent and non-violent Islamism or jihadism over the course of one month.[8]

[5] For example, according to Sir Norman Bettison, the former chief constable of West Yorkshire Police and the Association of Chief Police Officers (ACPO) lead on the government's *Prevent* strategy, "The internet features in most, but not all, terrorism cases." See Home Affairs Committee, *Roots of Violent Radicalisation*, London: January 2012, http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144602.htm.

[6] Ines von Behr, Anais Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism,* RAND Europe, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

[7] Jacques Bughin, Laura Corb, James Manyika, Olivia Nottebohm, Michael Chui, Borja de Muller Barbat, and Remi Said, *The Impact of Internet Technologies: Search – July 2011*, McKinsey & Company High Tech Practice, July 2011, https://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/High%20Tech/PDFs/Impact_of_Internet_technologies_search_final2.ashx

[8] For a partial list of keywords see Appendix.

By analysing the search frequencies, we confirmed which of the 147 keywords were the most commonly used. We then analysed two samples totalling 47 keywords. The keywords with the highest monthly average search frequencies in the UK were selected for the first sample and keywords that carried a higher potential of risk, in regards to extremist content, were selected for the second. We looked at the first two pages of results generated by those keyword searches and categorised the nature of the content they led to. Through this, we were able to assert which keywords generated extremist content, and whether the search results featured any counter-narratives to challenge them.

Keyword searches are the way in which we access the world wide web. Our analysis reveals how easily the average user can come across extremist content through simple searches in Google. Most importantly, it shows the wide array of keyword searches that generate radical lectures, violent fatwas, and access to jihadi manuals. According to our findings, not just overtly violent language or jihadi vocabulary generates extremist material; otherwise benign, apolitical, and non-violent language also facilitates access to websites promoting violence. In light of the most concerning results from our research, we suggest that increasing the prominence of counter-narrative content for relevant keyword searches should be used as a first line of defence against extremist content online.

Our analysis of keywords and their search results also showed how often extremist content dominates counter-narratives online. The findings suggest an urgent need to redress the balance of content for Google searches of particular keywords.

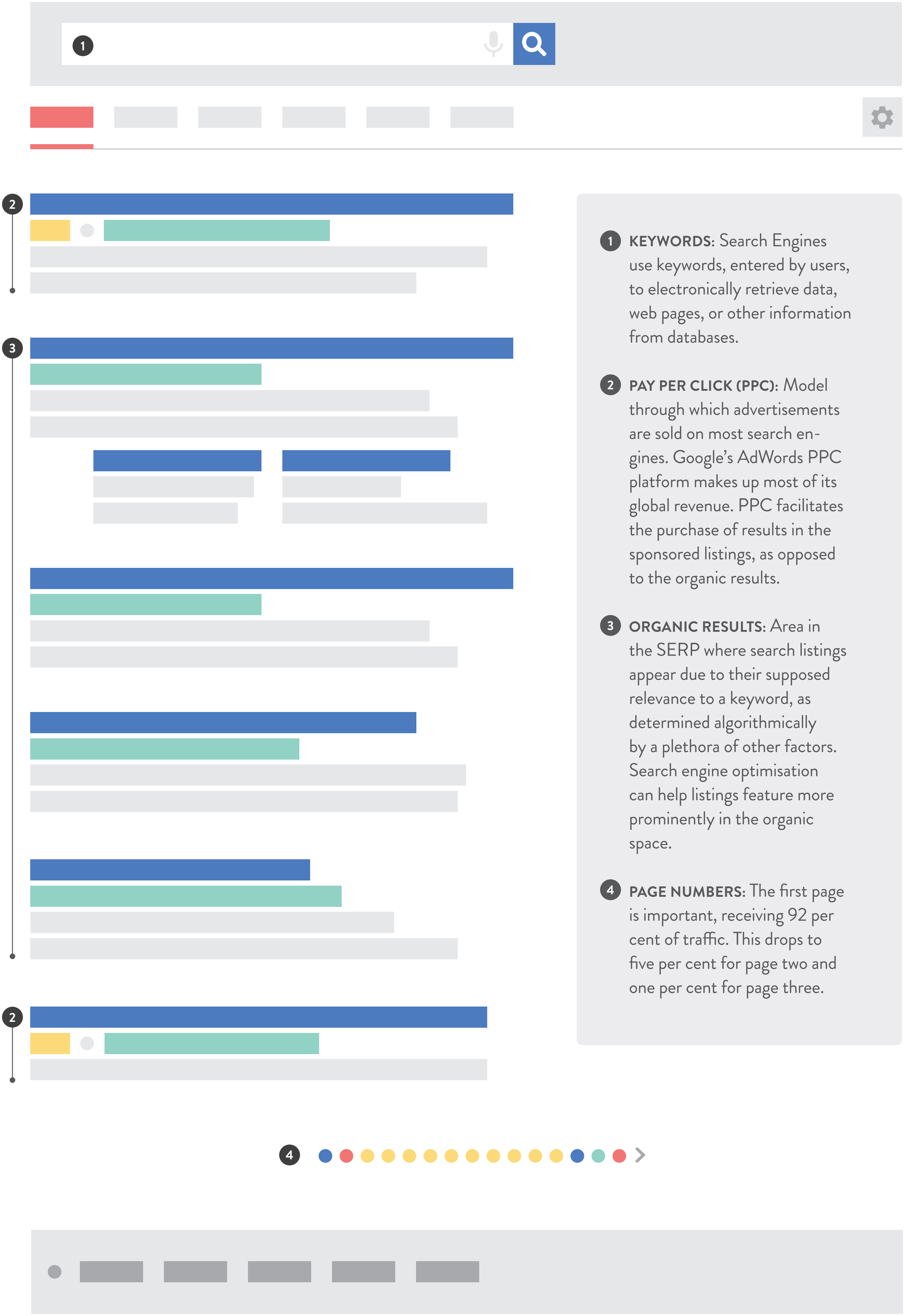
When it comes to websites, appearances can be deceiving. We came across extremist material on otherwise mainstream reference sites and the sites of non-violent Islamist groups. Understanding this is crucial to addressing how easy it can be to access extremist content online. Forty-four per cent of the extremist material identified as readily available via simple Google searches was explicitly violent.

This study provides a snapshot of the vast array of extremist content online, and how easy it is to access. By bringing together the technical expertise of Digitalis Reputation and the Centre on Religion & Geopolitics (CRG)'s knowledge of extremist ideology, this report provides a diagnosis of the state of play of extremism online. It also tells us about the successes and failures of online counter-narrative efforts.

Those working to make the world wide web a safe space need to understand the technical and ideological issues surrounding extremist content on the internet. As such, this study aims to provide a useful resource for governments, technology companies, and civil society groups working to counter extremism.

FIG. 1.1 Layout of a Search Engine Results Page (SERP)

Important components when considering search results



1 **KEYWORDS:** Search Engines use keywords, entered by users, to electronically retrieve data, web pages, or other information from databases.

2 **PAY PER CLICK (PPC):** Model through which advertisements are sold on most search engines. Google's AdWords PPC platform makes up most of its global revenue. PPC facilitates the purchase of results in the sponsored listings, as opposed to the organic results.

3 **ORGANIC RESULTS:** Area in the SERP where search listings appear due to their supposed relevance to a keyword, as determined algorithmically by a plethora of other factors. Search engine optimisation can help listings feature more prominently in the organic space.

4 **PAGE NUMBERS:** The first page is important, receiving 92 per cent of traffic. This drops to five per cent for page two and one per cent for page three.

PART TWO

Is Online Extremism Limited to Social Media?

Recent studies into online extremism have focused almost exclusively on the role of social media platforms such as Facebook, Twitter, and Telegram. But research by the Centre on Religion & Geopolitics (CRG) and Digitalis has found there is more to extremism online than social media.

SEARCH VS. SOCIAL MEDIA

Social media allows anyone with the most basic knowledge of the internet to get online and engage with others. Social media has also been proven to create an echo chamber of like-minded peers.[9] At the stage where someone has followed a hashtag or joined a group, they have likely already shown openness to an idea. Search engines, not social media, tend to be the first port of call when users are looking for information. Further, many internet users are savvy when it comes to marketing on social media; search engines are seen as more trustworthy sources of information, according to the research.

Web searches are the most trusted source of information for most people. Last year, Google, the world's leading search engine, was named the third-most trusted company in the world.[10]

The *2016 Edelman Trust Barometer* findings concurred. Some 71 per cent of browsers use a search engine on a regular basis, compared to 67 per cent who use social media several times a week or more. While 63 per cent trust news and information in search engine results pages (SERPs), only 44 per cent trust the news and information they find on social media." [11] YouGov research commissioned by Digitalis supports this, as only a small proportion of the sample questioned claimed to trust information provided by Facebook or Twitter in the search results, five per cent and eight per cent respectively. The same research suggested that when selecting an information source from a SERP, 76 per cent would choose the organisation's website, 72 per cent national media, and 67 per cent would choose Wikipedia as a trusted source of information.[12]

In fact, the internet as a whole is like an echo chamber for extremism. There is no control of dangerous content on the SERPs. What gives us further cause for alarm is the fact that users might trust information and links in search results pages, even if that content is extreme.

An individual could be looking for information about their religion online and find themselves exposed to extremist views, possibly unknowingly. The difference between actively seeking extreme content and coming across it through innocent inquiry is slight. Yet, this small margin is the difference between a user who knows what information they need and one who trusts the information generated by search results.

Further, the linking data discovered by Digitalis technology showed evidence that websites containing extremist content boast numerous inbound links. Along with other factors, the number of links that lead into a site impacts its ranking on a results page, with well-linked websites more likely to feature prominently in the relevant SERP. This may be the result of search engine optimisation (SEO) or a natural interest, but the effect is the same. We discovered a host of such sites ranking highly in search engine results pages.

[9] Brian Barrett, "Your Facebook Echo Chamber Just Got A Whole Lot Louder," *Wired*, 29 June, 2016, http://www.wired.com/2016/06/facebook-embraces-news-feed-echo-chamber.

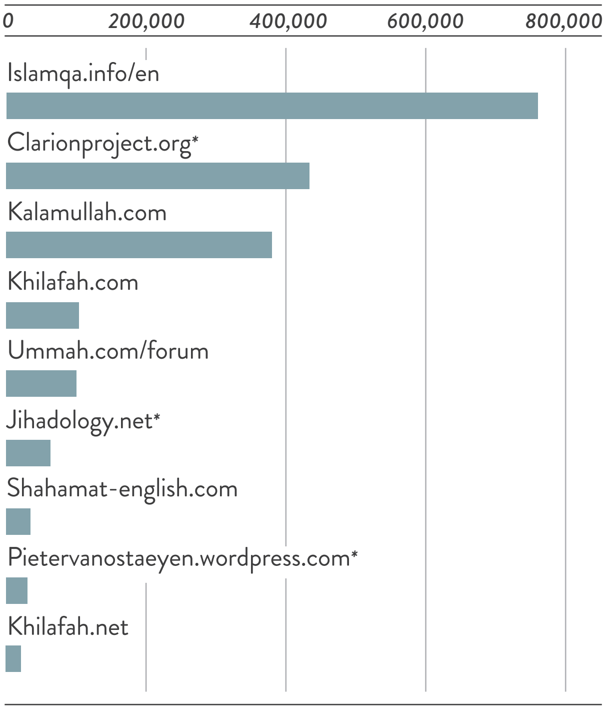
[10] Karsten Strauss, "The World's Most Reputable Companies," *Forbes*, 22 March, 2016, http://www.forbes.com/sites/karstenstrauss/2016/03/22/the-worlds-most-reputable-companies-2016/#211e77c4f952.

[11] This year social media received its lowest trust score in four years in the *Edelman Trust Barometer*. See *2016 Edelman Trust Barometer*, Edelman, January 2016, http://www.edelman.com/insights/intellectual-property/2016-edelman-trust-barometer/.

[12] *UK Opinion Formers Omnibus*, YouGov PLC, April 2015 (sample size 790).

FIG. 2.1 Links Entering into Sites Found to Contain Extreme Content

By total number of links



** Contains extremist content for research and analysis purposes.*

CASE STUDY

Search Engine Optimisation

SEO (Search Engine Optimisation) is the now all but ubiquitous science of promoting one's website in order to enhance its ranking in search engines for relevant phrases – often the generic searches for products an organisation sells.

Google's ranking algorithm takes account of a reported 200 different factors in determining the relevance of one site relative to another for a specific search phrase. In recent years, the volume (and relative quality) of other sites which link into the site in question has been of increasing relevance. Essentially, Google considers that if many people are linking to or referencing a particular article then it must be of more interest than an article which nobody mentions. Most recently, consideration of these 'inbound links,' their quantity and quality, has been broadened to incorporate what Google refers to as 'social signals.' This might include Facebook Likes, Tweets or Retweets, and the like.

As a result, link building has become a key pillar of SEO work: the more links (natural or otherwise) into a specific site, the higher it might rank on search engine results pages (SERPs) for its target keywords. Creating the appearance of grassroots support for a news article or website can artificially enhance its ranking in search engines.

In consumer sectors with tough competition such as credit cards, mobile phones, and other retail categories, the ability to make rapid gains in SEO no longer exists. In the battle for ideas online, however, few organisations are putting up a sophisticated fight. As a result, offensive material, if naturally discussed by many and certainly if deliberately promoted through sophisticated SEO, will often rank prominently.

The online library Kalamullah.com, which contains literature and sermons from prominent jihadi figures, has 378,169 links into it from other sites, for instance. Meanwhile, Khilafa.com, the official international English website of Hizb ut-Tahrir, a caliphate-supporting, anti-Western group, has 103,567 links. In comparison with the sites we analysed that offered counter-narratives, websites with extremist content had a larger number of links into them. This meant they typically had a stronger online presence in the SERPs.

Online extremism is clearly not just about social media. Refusal to engage with the broader online landscape has created a blind spot that extremist sites – some managed by individuals who appear to understand the principles of SEO – are taking advantage of. This is in stark contrast to the British government's own counter-extremism strategy, *Prevent*, which states "there should be no 'ungoverned spaces' in which extremism is allowed to flourish."[13]

Extremists online are widely misunderstood as technologically sophisticated and highly savvy when it comes to the internet. But they are simply products of their time. It is important to recognise that their success online is not necessarily a matter of technological sophistication.

Extremist content, in its various forms, exists online and is readily available on websites. A user can come across it while browsing for Islamic literature or during a forum discussion. It was concerning to discover that extreme content is present in the SERPs for a variety of keywords, some of which are not overtly extreme.[14]

The content found was varied. Extremist material features in online publications, forums, videos, clearing sites, and official websites, from violent and non-violent to political Islamist. We need to ask questions about how extremist content has managed to be promoted so successfully on the internet. Where, if at all, does the responsibility for online control lie?

[13] HM Government, *Prevent Strategy*, London: June 2011, p.9, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

[14] Examples of such keywords include 'caliphate' and 'apostasy.' For a fuller list see Appendix.

TERMS

Extremist Content Types

Extreme, Violent: Explicit depictions of graphic violence or exhortations to carry out acts of violence. Examples include websites and content in support of ISIS, al-Qaeda, and other jihadi groups.

Extreme, Non-Violent: Sectarian, racist, anti-Semitic, homophobic, and other offensive content, but with no explicit depiction or exhortation to commit acts of violence. For example, ideas expressed by Salafi and other puritanical Islamic groups.

Political Islamist: Non-violent content that is specifically politically motivated from and expressed by, or in support of, known political Islamist groups. In addition to the criteria of non-violent content, political Islamist content expresses the need to replace existing systems of governance and replace them with an Islamic system in which the Sharia is the dominant legislation. This includes groups like the Muslim Brotherhood, Hamas, and Hizb ut-Tahrir.

MANY DOORS TO EXTREMISM ONLINE

It is safe to assume that today, with access to the internet continuing to grow, people looking for information about a host of subjects, including Islam, will start their journey with an online search.

Google holds 89 per cent of the global market share in search engines;[15] the vast majority of searches will start there. Eighty-two per cent of internet users begin their search with Google,[16] and 90 per cent of internet users navigate the internet using search engines.[17] With 40,000 searches a second, 2.5 billion a day, and 1.2 trillion per year worldwide,[18] Google is the lifeblood of online searches.

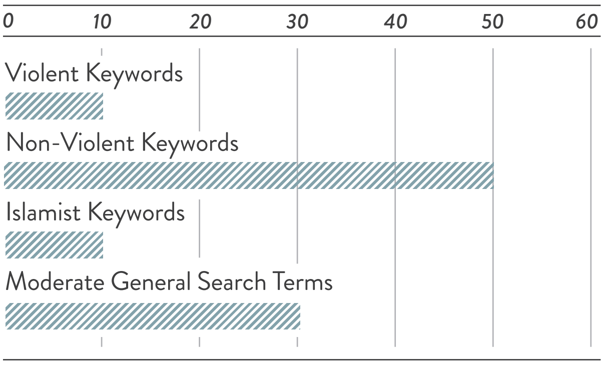
Keywords are crucial when looking for information online as they give access to content on the SERPs. By understanding which keywords return extremist content and by analysing their search frequencies we are able to gain an insight into the accessibility of extremist content. We may hope that the keywords used to access extremist content through online searches will be obscure and only known to insiders. In order to explore this, this study focused on the 'most popular' keywords from our selected sample.

To understand the use of certain keywords, Digitalis and CRG created a list of 287 English and Arabic keywords that are potential gateways to extremism online. The frequency with which these are searched each month, globally and regionally, was then ascertained. Keywords with a monthly average search frequency of more than 500 were considered the 'most popular.' Of the 143 English keywords monitored, 23 (16 per cent) were searched on average at a minimum rate of 500 times per month. The SERPs of these most popular keywords were subsequently analysed.[19]

We categorised these 23 most popular keywords by ideological type. This allowed us to understand what type of keyword gave access to what type of content. In other words, was extreme content only returned in the SERP when using an explicitly extreme keyword? Or could non-extreme keywords also return extreme content in the SERP?

FIG. 2.2 Different Keyword Types That Allow Access to SERPs Weighted Towards Extremist Content

By percentage of 'most popular' sample



Our analysis of the results of these 23 keywords identified 11 SERPs that contained extremist content within the first two pages. All categories of keywords we recorded – violent, non-violent, Islamist, and moderate – led to some form of extremist content.

Given that we know the dangers of online radicalisation, extremist views should be difficult to find. However, it would appear that all categories of keyword in our study led to some type of extremist content.

The sheer popularity of these search terms means that extremist content is available to a very large number of peo-

[15] "Worldwide Desktop Market Share of Leading Search Engines from January 2010 to January 2016," *Statista*, http://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.

[16] This data is for Google only and does not include other search engines. See Nielsen MegaView, August 2010; Internal Google Data from February-July 2010 vs. February-July 2011; comScore, June 2011 in Blerina Sanocki, "Introduction to Online Search: Best Practices for Leveraging Online Marketing to Grow your Business," presentation, http://www.acg.org/UserFiles/file/newjersey/Search101%20for%20ACG%20Summit-Blerina%20Sanocki.pdf.

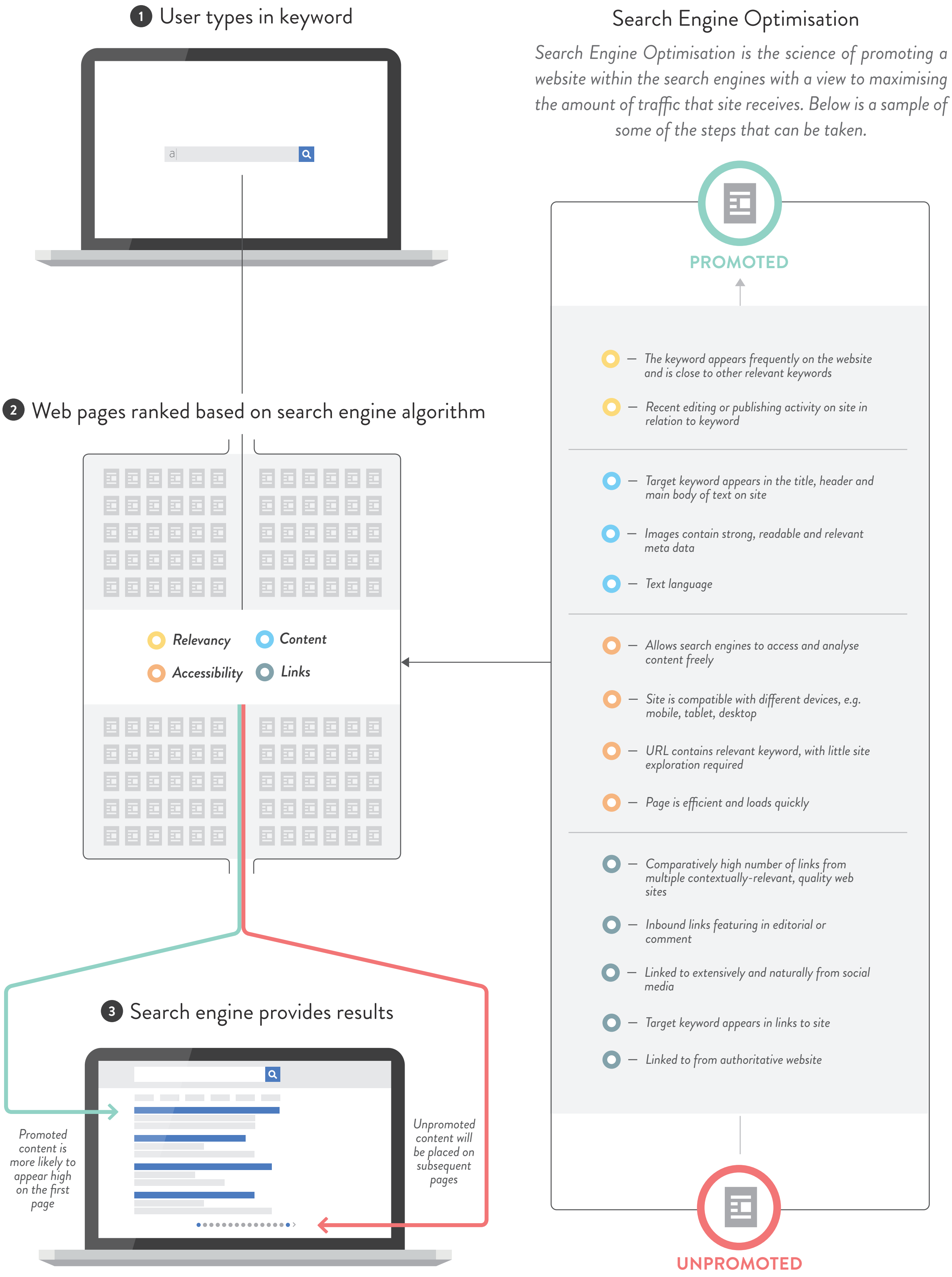
[17] Bughin et al, *The Impact of Internet Technologies.*

[18] "Google Search Statistics," www.internetlivestats.com/google-search-statisitcs.

[19] For list of most popular keywords see Appendix.

FIG. 2.3 An Overview of How Search Engines Rank Content

The basic principles that govern how Google returns and ranks content based on a keyword search.



1 User types in keyword

2 Web pages ranked based on search engine algorithm

- ○ *Relevancy*
- ○ *Content*
- ○ *Accessibility*
- ○ *Links*

3 Search engine provides results

Promoted content is more likely to appear high on the first page

Unpromoted content will be placed on subsequent pages

Search Engine Optimisation

Search Engine Optimisation is the science of promoting a website within the search engines with a view to maximising the amount of traffic that site receives. Below is a sample of some of the steps that can be taken.

PROMOTED

- ○ — *The keyword appears frequently on the website and is close to other relevant keywords*
- ○ — *Recent editing or publishing activity on site in relation to keyword*

- ○ — *Target keyword appears in the title, header and main body of text on site*
- ○ — *Images contain strong, readable and relevant meta data*
- ○ — *Text language*

- ○ — *Allows search engines to access and analyse content freely*
- ○ — *Site is compatible with different devices, e.g. mobile, tablet, desktop*
- ○ — *URL contains relevant keyword, with little site exploration required*
- ○ — *Page is efficient and loads quickly*

- ○ — *Comparatively high number of links from multiple contextually-relevant, quality web sites*
- ○ — *Inbound links featuring in editorial or comment*
- ○ — *Linked to extensively and naturally from social media*
- ○ — *Target keyword appears in links to site*
- ○ — *Linked to from authoritative website*

UNPROMOTED

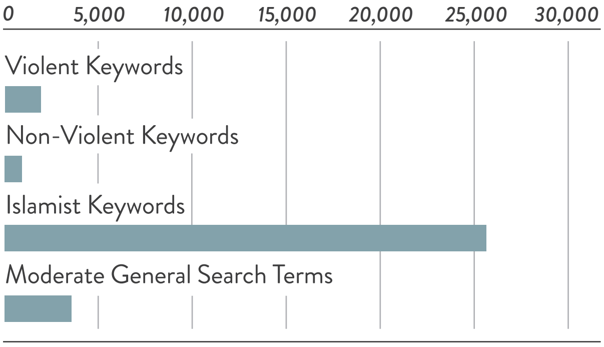
The above metrics and factors represent a selection only of the reported 200 factors which influence Google's algorithm (and the respective algorithms of other search engines).

ple. Forty-eight per cent (11) of our most popular keywords returned extremist content in their search page results. The search frequencies of these 11 keywords add up to more than 50,000 searches a month in the UK, and over 450,000 globally.

While this number may appear to be insignificant in the global context, it is important to understand that some of the most heinous terror attacks committed in the name of religion have been perpetrated by a handful of individuals. The level of harm that can be inflicted by a single individual is the very reason why keyword searches in the thousands, or hundreds of thousands returning extreme content need to be analysed with greater attention.

FIG. 2.4 Total Monthly Search Frequencies in the UK for Types of Keyword

Accumulated number from 'most popular' sample



Keywords entered into search engines are the way we access the world wide web. The management of results for popular keywords should be used as the first line of defence against exposure to radicalising content online. However, the data we gathered points to incredible ease of access to extremist material through an array of extreme and non-extreme keywords. Extremist content is in plain sight for anyone to see, analyse, discuss – and act upon.

CASE STUDY

Keywords: 'Mujahideen' and 'Beheadings'

The results for the historical term 'mujahideen' are an example of how easy it is to access extremist material via the search engine results pages. Although the word, which refers to those engaging in jihad, is not used exclusively by those searching for jihadi content, a Google search returns an al-Qaeda video on page one of the results pages, with no counter-narrative to its message. The YouTube clip in question glorifies al-Qaeda training and ideology. It features al-Qaeda militant Abu Yahya al-Libi urging people to participate in jihad. Arriving at this video is simple. A term like 'mujahideen' is embedded in history; the 33,100 searches on average a month globally should be free from extremist material. If a search for the Irish Republican Army or the West Side Boys returns documentaries and moderate narrative, why is content surrounding terms like 'mujahideen' still linked to extremist material?

There are some keywords that should already be targeted by counter-narratives because they provide unfettered access to extremist content. One example is a term like 'beheadings,' which is searched on average 12,100 times a month globally. Given the current trends of Islamist extremist groups executing captives by beheading, this search term carries a risk of generating search results with extremist material. Indeed, 'beheading' has extremist content in the SERPs – we identified six sites, presenting extremist content, all of which was violent.

Both 'mujahideen' and 'beheadings' are keywords that return extreme content in the search engine results page, however despite one being historically rooted and the other more prevalent today, both are no more than a Google search away.

THE ROLE OF CLEARING WEBSITES

Online clearing websites are places where analysts and researchers can access extremist content for research purposes. But with jihadi content so easily accessible on these sites, should more be done to protect vulnerable internet users from accessing them?

ISIS' English-language magazine *Dabiq*, for instance, and al-Qaeda in the Arabian Peninsula (AQAP)'s *Inspire* magazine, are both readily available to browse and download through clearing sites. UK courts have convicted defendants for possessing and distributing these magazines. Security concerns around such publications are clearly already on the agenda.[20]

Yet in the digital realm, there is little to no safeguarding in place when it comes to *Inspire*, *Dabiq*, and others. The objectives of these publications are clear: to recruit and 'guide' individuals onto the path of jihad. With this in mind, it seems not enough attention has been given to how easy it is to find them online.

Facebook, Twitter, and other platforms have been cited as

[20] Kashmira Gander, "ISIS: Bradford Man Jailed for Sharing Extremist Group's Dabiq Propaganda Magazine on his Facebook Page," *The Independent*, 24 April, 2015, http://www.independent.co.uk/news/uk/crime/isis-bradford-man-jailed-for-sharing-extremist-groups-dabiq-propaganda-magazine-on-facebook-10202642.html; Tom Whitehead, "Bride Jailed for Downloading Terror Magazine," The Telegraph, 6 December, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9727045/Bride-jailed-for-downloading-terror-magazine.html.

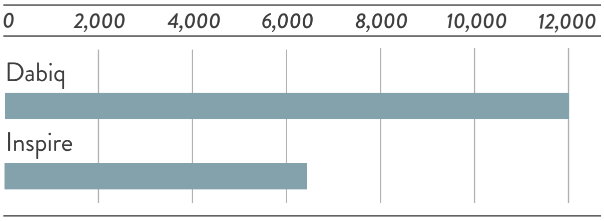
key to spreading jihadi content. At the same time, many other websites provide safe access to exactly the same content. A simple Google search for *Dabiq* or *Inspire* magazines is all that is needed to find the PDF versions of these jihadi publications. Should such sites not be subject to the same level of scrutiny as jihadi Twitter accounts?

In the online battle against ISIS, extremist material is removed from social media platforms; accounts of known jihadis are shut down and posts deleted. But even if links to online file sharing websites such as Archive.org are removed from Twitter and Facebook, the content they link to remains on clearing sites. Jihadology.net, a prominent clearing house blog for researchers, provides links to content hosted on Archive.org. These sites have an important role in helping understand the phenomenon of violent extremism, but we cannot ignore the fact that they make this content available to a wider audience. We need to accept that if analysts and researchers have such easy access to jihadi material, then all other internet users do too. Some of these people will be vulnerable to radicalisation.

With this in mind, efforts must be made to prevent such online content from being used by those with ulterior motives. Consideration must be given to requiring payment for access, conducting organisational and individual due diligence, or even the introduction of new legislation to ensure extreme content on clearing sites does not end up being utilised by jihadis as a safe storage space for their material.

FIG. 2.5 Global Searches for Extreme Islamist Magazines

Number of average monthly searches on Google



CASE STUDY

Following the Links: From Jihadology.net to an ISIS Site

The linking data for Jihadology.net, one of the most popular clearing sites for accessing jihadi content online, returned 61,793 links from 2,581 domains, which evidenced a strong online presence. Subsequently, Jihadology.net appears prominently within search results pages. A manual trawl through those links revealed that at least one jihadi website linked to this safe hosting of jihadi content. Even more worryingly, this jihadi site led to a portal for ISIS supporters in Europe.

The site in question, Islamenmelilla.blogspot.com, appears to be quite dated, but it still features content and links for hundreds of jihadi propaganda videos, nasheeds (chants/vocal music), texts, and other jihadi resources. There is no doubting the jihadi credentials of this website. Yet the link to Jihadology.net, which is clearly not a jihadi site, features quite prominently on Islamenmelilla.blogspot.com. In fact it bears the very same title image featured on Jihadology.net itself. The link is active. It takes the user to a webpage on the Jihadology.net website that is described in the URL in the address bar as 'Maktabah al-Jihadiyyah.' This is Arabic for 'The Jihadi Library.' While this page does not appear to host any extremist content under that URL, it does bring the user to Jihadology.net. From there, the user has unrestricted access to jihadi material.

Jihadology.net is a genuinely useful resource for those trying to understand jihadi ideology, but it does raise serious questions about hosting extremist content online, for whatever purpose. Ultimately, publications deemed illegal if downloaded or circulated by others offline are perfectly legal and stable on this website.[21]

Furthermore, when we explored Islamenmelilla.blogspot.com in more detail, we found that it linked to a gateway for European ISIS supporters. Via an antiquated and disorganised blog page on Islamenmelilla.blogspot.com, users could access Al-khelafa.eu. This site is entitled 'Ansar al-Khelafa Europe,' which translates as 'Supporters of the Caliphate Europe.' This closed forum site, decorated with the image of an ISIS flag draped over the European continent, contains 'official' news, images, publications, and broadcasts. It remained active as of July 2016.

[21] Ibid, p.23.

PART THREE

Is Online Extremism Limited to Jihadi Content?

VARIETY OF EXTREMIST CONTENT

The websites this study identified as hosting extremist content were an eclectic mix with a wide array of messages. As with the variety found in keyword categories that allowed access to extremism, extremist sites of varying types appeared in the search engine results pages (SERPs).

We found evidently extreme content in the first two pages of search engine results pages. No expert knowledge was required to access this material. From the SERP analysis we conducted, we analysed 870 web pages, 91 of which contained extremist content. This was only from analysing the SERPs of a sample of 47 keywords for pages one and two of the results.

The way in which we found extremist content points to a lack of content control and ease of accessibility. Furthermore, 44 per cent of the extremist content we identified, and that was readily available to the average user, was violent.

Extremist views are accessible online in a number of forms. When we analysed the SERPs, we saw that it was very simple to find extremist material on blogs or a political Islamist website, to read a PDF of the latest copy of a jihadi magazine, or to come face-to-face with an extremist ideology while innocently asking a question on a forum.

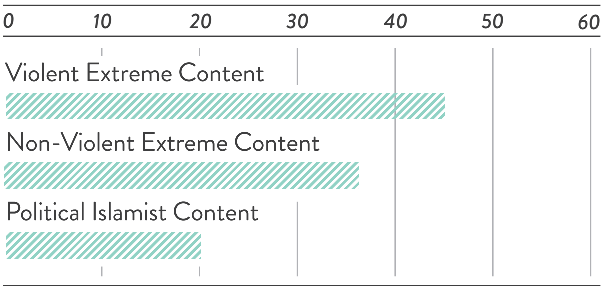
CASE STUDY

Keyword: 'Khilafah'

The results for the keyword 'khilafah' are a good example of how a wide array of sites contain extremist messaging. With nine extremist sites in the first two pages of the search engine results pages (SERPs) for a phrase with a search frequency in the UK of 880 per month, it shows how search results can be hijacked by an extremist message.

FIG. 3.1 Extreme Content Type Found

By percentage of sample



Ubiquitous on the SERP is Khilafah.com, the Hizb ut-Tahrir website, which expresses views such as "khilafah is the answer." This website presents the 'correct' organisational structure the Islamic caliphate should take, and repeatedly presents the West as negative and oppressive. The site currently ranks highly in search results, dominating the SERPs for the keyword 'khilafah.'

Also available on the SERPs for 'khilafah' is a YouTube video titled "The Forgotten Obligation" calling for a return to the caliphate, which features audio clips from Anwar al-Awlaki, a former ideologue for al-Qaeda in the Arabian Peninsula (AQAP).

Blogs can also be a platform for extremist voices. Ansarukhilafah.wordpress.com, which hosts content from and on behalf of ISIS, describes itself as "a must read for all the English speaking brothers; be they mujahideen (jihadi fighters) or munasireen (helpers/supporters)." This content is designed both for those seeking to fight for ISIS' so-called caliphate, and those supporting it from afar. Another more active blog, Islamicsystem.blogspot.com, contains a list of articles relating to the establishment of the caliphate. It expresses the view that "the desire for the return of the caliphate is not limited to a few militants as some attempt to portray, it is an essential part of Islam which every Islamic scholar in history has agreed upon."

With an extreme to counter-narrative ratio of 9:0, 'khilafah' clearly has an extremist-weighted SERP that is above average, but the variety of content available when you type that search term into Google gives a snapshot of the online landscape. It also shows how easy it is to access online extremist content. This is due in part to successful online campaigns by those communicating extremist views, which is further intensified by the dearth of counter-narratives.

▪

TYPES OF CONTENT ARE HARD TO DISTINGUISH

In recent years, governments, internet service providers, and technology firms have been criticised for not doing enough to fight extremism online, particularly in light of ISIS' prolific use of the internet for propaganda and recruitment. The removal of graphic violence and child pornography is a relatively straightforward task for tech companies because they are easier to identify. But extremist content spans a broad spectrum, with violent jihadis and political Islamists drawing from the same ideological framework from which many ordinary Muslims also draw. Some material crosses the line into extremism, and some has the potential to radicalise users.

The current designation of extremist content may easily identify images and videos, but may not necessarily pick up on the wealth of extremist publications and lectures that are accessible online, yet more difficult to identify as being extreme. To make matters even more complicated, many of these materials can be found on sites that could ordinarily be dismissed as harmless general Islamic websites.

Websites such as Kalamullah.com and WorldofIslam.info contain resources used by ordinary Muslims and those interested in Islam. They feature online versions of the Quran, collections of Hadith literature, and an array of Islamic books. However, a closer look at these sites reveals that hiding in plain sight are jihadi manuals, as well as audio lectures and nasheeds.[22]

In a similar vein, IslamQA.info, a Salafi-oriented website that issues fatwas, or religious rulings, clarifies the 'Islamic' perspective for readers on a wide range of issues. Along with opinions on the correct way to pray or the virtues of fasting during Ramadan are answers relating to jihad, apostasy, and Shia belief. Some of these are far from moderate.

Websites such as Kalamullah.com, WorldofIslam.info, and IslamQA.info are not inherently extreme, but they certainly host content and views that are extreme. The stamp of authenticity these websites give to extremist ideas is cause for concern. If an individual accepts the authority of a given website on how to pray or what constitutes halal food, they are more likely to accept the extremist ideas they find there, from applying the death penalty to apostates, to anti-Semitism.

Likewise, if websites give access to the Quran and Hadith literature, the very foundations of the Islamic faith, users may approach extremist content hosted there with the same level of certitude.

These examples show the nature and breadth of the challenge. If we focus on jihadi groups like al-Qaeda or ISIS and the social media accounts and websites they operate, we ignore the very ideological substance that gives them their sense of legitimacy. After all, the likes of ISIS and al-Qaeda present their worldview as based on genuine Islamic scholarship.

NAVIGATING THE LABYRINTH

Analysing website linking data helps us understand the intricate labyrinth of paths that lead in to sites, a cyclical process which helps bring further websites to light. WorldofIslam.info is one of the websites we discovered by identifying links to other sites. In addition to giving access to its own content, WorldofIslam.info provides a multitude of links to other pages. Many of these links appear to be quite mundane. They relate to the Quran, prayer times, halal food, and science. But on the very same page there are links to two websites that came up again and again in our research: Kalamullah.com and IslamQA.info.

These two are not exclusively extremist sites per se, but both host extremist content. Kalamullah.com hosts lectures by former al-Qaeda ideologue Anwar al-Awlaki, as well as books by Abdullah Azzam, the man credited with playing a central role in the emergence of al-Qaeda and the global jihadi movement. Meanwhile, other links on the WorldofIslam.info homepage lead to a Twitter account of al-Qaeda's Syrian affiliate, Jabhat al-Nusra. Twitter has removed the account, but this still gives a clear indication of the site's links to jihadi content.

Kalamullah.com is another interesting example of the tightly woven online fabric. Its vast repository of books, lectures, and nasheeds features content that is widely accepted as being extremist, side-by-side with mainstream religious texts, like the Quran and Hadith. We identified 378,167 links coming into this site, the overwhelming majority of which, 75 per cent, came from a single source: Ummah.com.

Ummah.com is one of the largest online Muslim forums. According to our research, both Muslims and non-Muslims visit the site to engage with others and get answers to questions about Islam. Its interactive format provides a platform for a plethora of voices, from the moderate to the extremist.

[22] Literally 'anthem,' nasheeds are vocal music in the form of rhythmic chanting often sung a cappella. Salafi-jihadi groups often use nasheed for motivational purposes, but they are also used in celebratory gatherings.

We found that 'question and answer' sites like Ummah.com and IslamQA.info often come up in results pages for a number of the keywords we used in the SERP analysis, which were identified as returning extreme results. The element of trust is an issue here. Not only does the user access extremist ideas through a legitimate search engine, but then the website in question presents itself as trustworthy, while hosting strands of the same extremist ideology held by jihadi groups.

Websites like Kalamullah.com and WorldofIslam.info, which host traditional Islamic content alongside extremist material are, whether knowingly or unknowingly, abusing the trust of their readers. The lines between religious conservatism and violent and non-violent extremism can grow increasingly thin as a result. Users who do not have the knowledge to tell the difference between the two may fall prey to this extremist content.

These examples are merely the tip of the iceberg, given the vastness of the internet. But they highlight the need to explore not only the content of specific sites, but also the links into and out of them. If we focus more on this, we will be able to better diagnose the scale of the challenge and more importantly, better equip those working to counter extremism online.

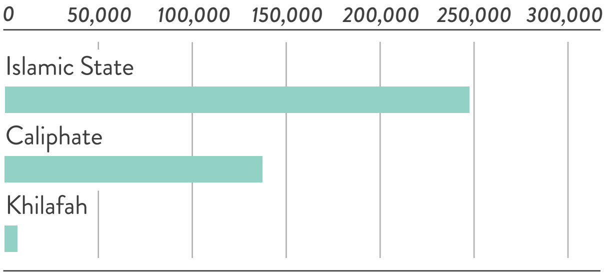
HIZB UT-TAHRIR

The main difference between ISIS and other Salafi-jihadi groups is its establishment of a caliphate. In propaganda, ISIS presents its caliphate as the legitimate, Islamic system of governance. This so-called caliphate, ISIS claims, is in accordance with religious scripture, it unifies the Muslim world and fights for its defence. The caliphate is a key pillar of ISIS' global appeal. When the group announced the caliphate in July 2014, the flow of foreign fighters to ISIS in Iraq and Syria increased significantly.[23]

Given the international attention and extensive media coverage on the so-called 'caliphate,' it is hardly surprising that our data showed an average of 135,000 global monthly searches for the keyword 'caliphate.' The transliterated English keyword 'khilafah', Arabic for caliphate, on the other hand has far fewer monthly searches globally, just under 10,000. 'Khilafah' is a far more niche search term. It is more synonymous with the Arabic and Islamic roots from which the concept of the caliphate stems. Despite conceptually referring to exactly the same idea, the anglicised word 'caliphate' demonstrates significantly more searches than the transliteration of the Arabic 'khilafah.' While not all searches for these concepts will necessarily be referring to ISIS, the term 'khilafah' is very much a part of ISIS' institutional vocabulary.

FIG. 3.2 Comparative Searches Related to the Islamic State

Number of average monthly searches on Google



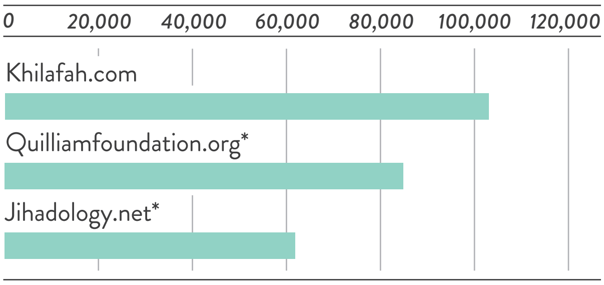
Search results for either 'caliphate' or 'khilafah' do not bring up content produced by ISIS. However, the latter is dominated by another Islamist group with the same ambitions. Hizb ut-Tahrir, a global pan-Islamic movement founded in 1953, also seeks to establish an Islamic state governed by sharia law and led by a caliph. While Hizb ut-Tahrir has condemned acts of terror and insists it follows a non-violent approach, it has supported military coups and shares much of ISIS' worldview. Establishing an Islamic state and a caliphate are central ideas for both groups. In theory, the only difference between Hizb ut-Tahrir and ISIS are the means of achieving these ambitions, but both advocate for an Islamic state. While the objective of the study was to discover the breadth of extremist content available through the SERPs, it was an unexpected discovery that the evidence revealed such a strong showing for Hizb ut-Tahrir.

Hizb ut-Tahrir has an incredibly robust online presence. Searches for 'khilafah' return high-ranking pages from the Khilafah.com website at the top of the SERP, including the official central website operated by Hizb ut-Tahrir, some of the group's country-specific sites, and other unofficial blogs supporting the group.

Along with various other factors, websites gain prominence in search result rankings from the number and strength of websites that link into them. This relationship, whether organic or engineered by people with search engine optimisation (SEO) expertise, supports a site in outperforming others.

FIG. 3.3 Links Entering Into Khilafah.com and Compared to Other Leading Websites

By number



* *Not extremist websites.*

[23] Hardin Lang and Muath al-Wari, *The Flow of Foreign Fighters to the Islamic State*, Center for American Progress, Washington DC: March 2016, p. 19, https://cdn.americanprogress.org/wp-content/uploads/2016/03/17132821/ForeignFighters-report.pdf.

If we compare Khilafah.com, the official website of Hizb ut-Tahrir, with other major sites in the counter-extremism field, its strong online presence is clear. Khilafah.com has more links directing to it than many leading analysis and counter-extremism sites. There are a number of variables at play in promoting results up the search engine rankings, but linking goes a long way.

WHY IS THIS A CONCERN?

There may be operational differences between Hizb ut-Tahrir and ISIS, but both derive from the same ideological framework. Islamists range from the democratically engaged to those who oppose democracy, from those using infiltration methods, like Hizb ut-Tahrir, to those employing acts of terrorism, like ISIS. What they share is an ideology that seeks to establish some form of Islamic governance and to implement their interpretation of Sharia law as state law.

The idea that individuals move along a 'conveyor belt' from non-violent Islamist groups to fully-fledged jihadis ignores the many factors that send someone on the path to militancy. However, research from the Centre on Religion & Geopolitics (CRG) has shown there is a closer link between the two than some may like to admit. According to CRG data, 51 per cent of prominent jihadis had been involved in non-violent Islamist organisations prior to their involvement in jihad.[24] This indicates that, in some cases, buying into the worldview of Islamist groups may lay the ideological foundation for those who go on to adopt the jihadi movement's narrower interpretations of Islam.

FIG. 3.4 Searches Globally and in the UK for Keywords Related to Islamism

Number of average monthly searches on Google

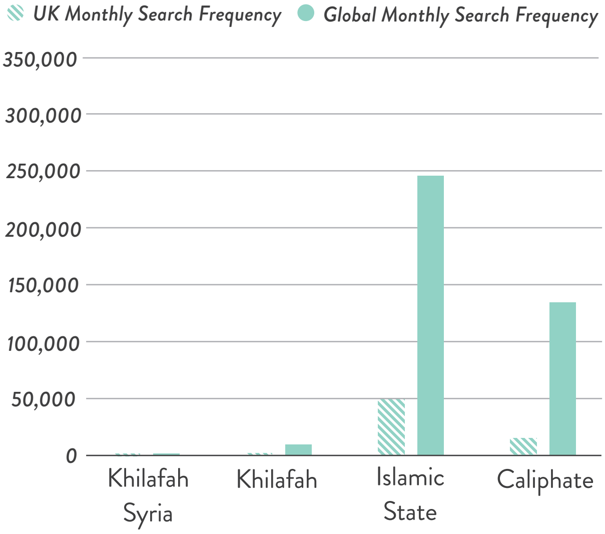


TABLE 3.1 Nature of Content in the SERPs

Amount of content found

Keyword	Extreme	Counter-Narrative	Neutral
Islamic State	0	0	18
Caliphate	1	0	18
Khilafah	9	0	10
Khilafah Syria	12	0	7

SEARCH ENGINE RESULTS PAGE ANALYSIS

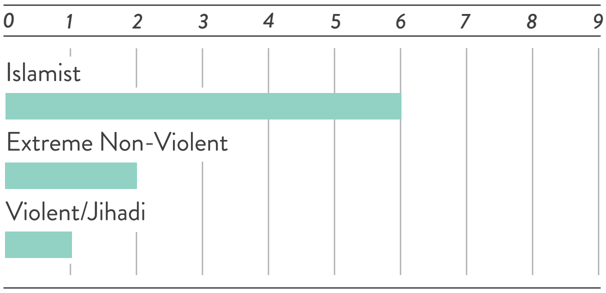
SERP analysis shows that for searches under the terms 'khilafah' and 'khilafah Syria,' the user is presented with results where extremist content dominates counter-narrative content, the majority of which is either from Hizb ut-Tahrir, or in support of it.

For the search term 'khilafah,' which has almost 10,000 global monthly searches, the ratio of extreme content to counter-narrative is 9:0.[25] No identifiable counter-narrative presents a more nuanced understanding and context for the concept of the caliphate. While for 'khilafah Syria,' a pertinent search term given that ISIS has established its caliphate partly in that country, the ratio is 12:0 in favour of extremist material.

In both cases there is an absence of counter-narratives to challenge the worldview and ideology put forward by extremists online. Websites promoting extremist ideas are left unchallenged. There are no safeguards in place.

FIG. 3.5 Extreme Content Type for 'Khilafah'

Total number found

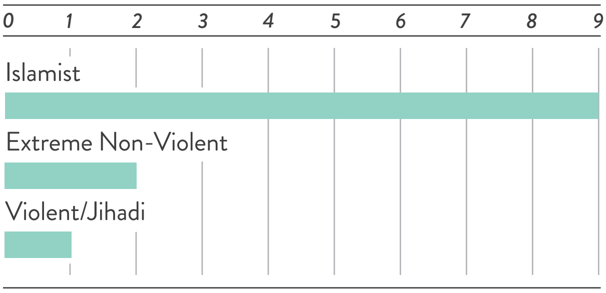


[24] Mubaraz Ahmed, Milo Comerford, and Emman El-Badawy, *Milestones to Militancy*, Centre on Religion & Geopolitics, London: April 2016, http://tonyblairfaithfoundation.org/sites/default/files/Milestones-to-Militancy.pdf.

[25] These ratios have been used to illustrate the comparison between extremist content and counter-narrative content found in the first two pages of search engine results pages, showing extreme content: counter-narrative content. Neutral content is ignored in these ratios.

FIG. 3.6 Extreme Content Type for 'Khilafah Syria'

Total number found



CASE STUDY

Extremist Content: Ansarukhilafah.wordpress.com

A Wordpress blog titled "Ansaru Khilafah" appears on the first results page for the search term 'khilafah,' which suggests it has a strong online presence. The blog gives access to a wealth of jihadi content – and does little to hide this fact.

This blog, clearly still active according to the dates of the most recent content updates, hosts much pro-ISIS material. This includes theological 'proofs' confirming the validity of ISIS' caliphate, refutations of its rival jihadi groups, transcripts of statements by senior ISIS figures, and security tips on how to remain undetected online while browsing extremist content.

The blog is not an official ISIS outlet, rather a page created by sympathisers, as is suggested from the name Ansaru Khilafah, which translates as 'servants or helpers of the caliphate.' Nevertheless, it is very easy to access this website and the extremist content it hosts through a simple keyword search.

IS HIZB UT-TAHRIR EXTREME?

If Hizb ut-Tahrir is non-violent, is its content a problem in and of itself? On its UK site, the group outlines its requirements for establishing a caliphate. Among the conditions stipulated are that the caliph "must be contracted to rule by Islam only"[26] and that "the land must have external security in the hands of the Muslims alone, such that the Khilafah has the capacity to maintain its borders."[27]

The Khilafah.com website describes how "establishing the Khilafah and appointing the [Khalifah] is obligatory on all Muslims in the world, male and female."[28] Its establishment, the site argues, will end "years of oppression by some of the worst tyrants this world has ever seen."[29]

Hizb ut-Tahrir's online material has a conspiratorial tone. It suggests that the current situation in Syria "is a Western conspiracy to prevent the fall of America's agent in Syria, Bashar al-Assad, and the rise of the Khilafah (Caliphate) on the Method of the Prophethood in the place of his evil, Kufr [sic] rule."[30]

In describing the long term objectives of the group's vision of a caliphate, the site says that "the Khilafah is an expansionist state but does not conquer new lands in order to steal their wealth and resources."[31]

Hizb ut-Tahrir condemned terrorist attacks like those of 9/11 in New York and 7/7 in London. But what becomes apparent from these statements, taken directly from its website, is the group's ideological affinity with ISIS and al-Qaeda. Both ISIS and Hizb ut-Tahrir declare that the only system of governance should be the caliphate and that the only legislation should be the sharia. Both divide the world into Muslims and nonbelievers.

When it comes to Hizb ut-Tahrir's commentary on the Syrian conflict, the waters between violent and non-violent Islamism become even murkier. Headlines like "Only Khilafah Rashida Can Return Safety and Security to the Children of Syria"[32] and "Syrian Regime's Security Truce in Munich is the Bloody and Fatal Scheming of America and Russia,"[33] further demonstrate how close Hizb ut-Tahrir's worldview really is to that of ISIS.

Despite its non-violent stance, an offshoot of Hizb ut-Tahrir, al-Muhajiroun, which has been proscribed as a terrorist organisation in the UK, has been no stranger to acts of violence. A study found that almost half of all terrorist plots

[26] "The Obligatory Conditions for a Khilafah," *Hizb ut-Tahrir UK*, July 2014, http://www.hizb.org.uk/islamic-culture/the-obligatory-conditions-for-a-khilafah.

[27] Ibid.

[28] "What is the Khilafah? (Caliphate)," *The Khilafah*, http://www.khilafah.com/what-is-the-khilafah-caliphate.

[29] Ibid.

[30] Media Office of Hizb ut-Tahrir in Wilayah Pakistan, "Expose the Western Conspiracy to Prevent the Return of the Khilafah on the Method of the Prophethood in Syria," *The Khilafah*, 10 March, 2016, http://www.khilafah.com/expose-the-western-conspiracy-to-prevent-the-return-of-the-khilafah-caliphate-on-the-method-of-the-prophethood-in-syria.

[31] "What is the Khilafah? (Caliphate)," *The Khilafah*, http://www.khilafah.com/what-is-the-khilafah-caliphate.

[32] Tsuroyya Amal Yasna, "Only Khilafah Rashida Can Return Safety and Security to the Children of Syria," *The Khilafah*, 21 March, 2016, http://www.khilafah.com/only-khilafah-rashida-can-return-safety-and-security-to-the-children-of-syria.

[33] "Syrian Regime's Security Truce in Munich is the Bloody and Fatal Scheming of America and Russia," *The Khilafah*, 27 February, 2016, http://www.khilafah.com/regimes-security-truce-in-munich-is-the-bloody-and-fatal-scheming-of-america-followed-by-russia-making-the-revolutionaries-insecure-and-even-fight-under-the-pretext-of-who-is-the-terrorist-i.

and attacks in the UK, including the murder of Fusilier Lee Rigby in 2013 and the 7/7 bombings in London, could be traced back to al-Muhajiroun.[34]

CASE STUDY

Governments Against Hizb ut-Tahrir

Governments around the world have made efforts to curb the activities of Hizb ut-Tahrir, which suggests there is a widespread understanding that the group poses some degree of danger.

In the UK, former Prime Minister Tony Blair looked into banning the group shortly after the 7/7 attacks in 2005, part of a 12-point strategy to counter Islamist extremism. He was dissuaded by counter-terror advisors who said the ban would aid the group's recruitment efforts.[35]

Former Prime Minister David Cameron also said he would "ban any organisation which advocates hate or the violent overthrow of our society, such as Hizb ut-Tahrir."[36] However, these attempts were also unsuccessful; the UK's counter-terrorism watchdog recommended that the government back down on this Conservative Party manifesto pledge.

Other European countries, including Denmark, Germany, and the Netherlands have sought to take action against the group. In Russia, Hizb ut-Tahrir was officially outlawed in 2003, having been designated a terrorist organisation.[37]

There is just as much concern about Hizb ut-Tahrir in the Muslim world. With the exception of Lebanon, the United Arab Emirates, and Yemen, the group has been proscribed across much of the Arab world. The group has also been banned in other Muslim majority countries like Pakistan and Bangladesh.

In March 2016, Hizb ut-Tahrir held an event in Istanbul titled "International Khilafah Conference," which drew speakers from around the world. With a spectrum of jihadi groups battling in the Syrian conflict next door, one prominent Hizb ut-Tahrir speaker from Australia called on his peers to "lead the armies of jihad that will conquer Europe and America." The speaker, the head of Hizb ut-Tahrir Australia, Sheik Ismail al-Wahwah, also described NATO, Europe, and the US as "enemies" who "hate your religion, your Mohammad, your Quran." They need to be "dealt" with, he said, before they start "dealing with you."[38]

THE THREAT

What we are seeing with websites run by, or in support of, Hizb ut-Tahrir is a strong online narrative that echoes the same fundamental ideological points as ISIS. However, the group is free to operate in the online space, unchallenged. If individuals begin to accept the extremist, conspiratorial, and divisive worldview put forward by groups like Hizb ut-Tahrir, the only distinction between it and groups like ISIS is violence. In other words, Hizb ut-Tahrir's vision may lay the foundation for the radicalisation of individuals online. These individuals may become more susceptible to violent interpretations of the same ideology Hizb ut-Tahrir peddles.

GREY AREAS

Our research shows that though violent and non-violent Islamist groups may operate differently, the difference between their ideology online is not clearly delineated.

A narrow definition of online extremism, limited to groups like ISIS and graphic, violent content alone, would ignore groups like Hizb ut-Tahrir, which have a strong online presence and clout with users. To get to grips with the extent of extremist content online, we urgently need to understand what constitutes extremist content, and to acknowledge the danger it poses.

[34] Loulla-Mae Eleftheriou-Smith, "Radical Islamist Group al-Muhajiroun Linked to Half of British Terror Attacks in Past 20 Years," *The Independent*, 23 March, 2015, http://www.independent.co.uk/news/uk/crime/radical-islamist-group-al-muhajiroun-linked-to-half-of-british-terror-attacks-in-past-20-years-10128492.html.

[35] Jamie Doward and Gaby Hinsliff, "PM Shelves Islamic Group Ban," *The Guardian*, 24 December, 2006, https://www.theguardian.com/world/2006/dec/24/religion.uk.

[36] Shiv Malik, "Watchdog Recommends Tory U-turn on Banning Hizb ut-Tahrir," *The Guardian*, 18 July, 2011, http://www.theguardian.com/politics/2011/jul/18/watchdog-tory-uturn-hizb-ut-tahrir-ban.

[37] Mairbek Vatchagaev, "Russian Authorities Launch Crackdown on Hizb ut-Tahrir," *The Jamestown Foundation*, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=44517&tx_ttnews%5BbackPid%5D=7&cHash=4946dc55adebee86d80441294d8acde9#.V2J7zpMrJhE.

[38] Andrew Bolt, "Australian Sheik Calls for 'Armies of Jihad' to Conquer West," *Herald Sun*, 14 April, 2016, http://blogs.news.com.au/heraldsun/andrewbolt/index.php/heraldsun/comments/australian_sheik_calls_for_armies_of_jihad_to_conquer_west/.

PART FOUR

What Do Keyword Search Frequencies Tell Us?

Despite the best efforts of its rivals, Google has been, and will likely continue to be, the de-facto search engine for most of the world's internet users. Understanding global search habits and trends is by no means a new endeavour. Companies and organisations worldwide have invested heavily in this area to better understand their consumers, using analytics data, and following online developments to help better inform business decisions.[39] But, to date, these research methods have not been used to inform counter-extremism efforts.

As is symptomatic of the entire counter-extremism field, initiatives aimed at countering the tide of extremist content have simply not demonstrated the same degree of agility as extremists.

By following developments in Islamist extremism both on- and offline, counter-extremism practitioners, whether governments, technology companies, or civil society groups, can better understand which aspects of these ideologies are prevalent, and where. This will, in turn, better inform and guide the fight against extremism.

The bulk of this study has focused on the experience of the average internet user who may be interested in concepts relating to Islamist extremism. As such, it has concentrated on English material. As has been debated in counter-extremism fields, the factors that draw individuals towards extremist religious ideologies vary in different contexts. Modern technology enables us to look at the online searches being carried out in specific regions and analyse what the results tell us about the extremist narrative that is prominent in different parts of the world.

WHY ANALYSE SEARCH TERMS?

Data on keyword search frequencies can give insight into the search habits and tendencies of users over a given period, or in relation to a particular keyword. While the possession of such data is not new, sharing it with governments, civil society groups, and even technology firms may help ideology and counter-extremism experts work together with online marketing experts to better understand online trends and user behaviour.

Knowing which keywords are being used in a particular city, country, or region, equips counter-extremism practitioners with a greater understanding of the specific aspects of extremist ideologies that people search for in a given geographical area. It provides direction on how to construct more targeted counter-narratives.

For example, knowing whether there are a greater number of searches for 'jihad' in the UK than in the US can help us identify gaps in knowledge that may exist among search engine users and see where people searching for this keyword are located. Identifying trends like these is essential, not only for bolstering our understanding of extremist activity online, but also to make sure counter-measures are applied in relevant areas.

Identifying patterns in search term use can also give an indication of emerging ideological trends. Knowing which political Islamist concepts are searched for in a particular region gives us a user-generated snapshot of online extremism. With this in mind, counter-narratives can target specific aspects of extremist ideology, rather than using a 'one size fits all' approach.

Whilst a search term is not an indication of a user's extremist tendencies, the frequency of keywords can tell us whether there is interest in an issue or subject related to extremism.

While regional breakdowns could be misleading without demographic context, search frequency numbers can still give

[39] Benjamin Spiegel, "The Google Trends Data Goldmine," *Marketing Land*, 10 February, 2015, http://marketingland.com/google-trend-goldmine-117626; *The Growing Power of Consumer: Deloitte Consumer Review*, Deloitte, May 2014, http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/consumer-review-8-the-growing-power-of-consumers.pdf.

a good, rough estimate of how many people are searching for a particular keyword around the world. This gives an indication of how many users might be at risk of encountering extremist content online.

UNDERSTANDING JIHAD

FIG. 4.1 Global Searches for 'Jihad' in Arabic and English

Number of average monthly searches on Google

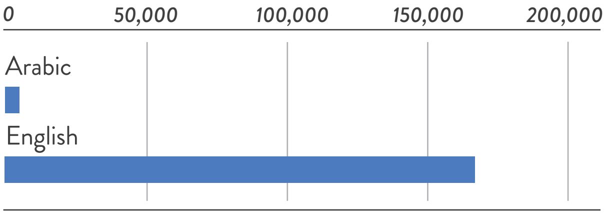
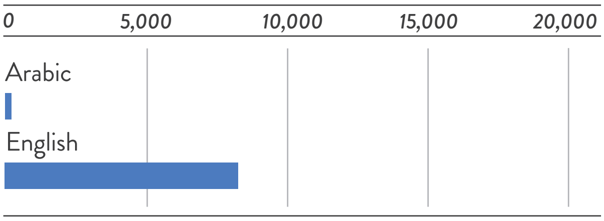


FIG. 4.2 Global Searches for 'Meaning of Jihad' in Arabic and English

Number of average monthly searches on Google



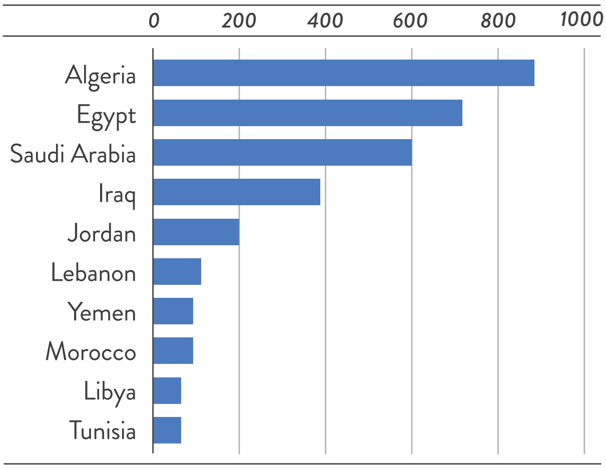
The media's frequent use of the word 'jihad' following the 9/11 attacks in 2001 has made the term a regular fixture of modern English vocabulary.[40] Globally, there are on average 165,000 Google searches per month for the term 'jihad' in English, compared to 6,600 in Arabic.

The disparity between the number of searches in each language is not entirely a surprise. The concept of jihad, which in some Muslim circles is described as the sixth pillar of Islam,[41] occupies a prominent place in the religious sentiments of all Muslims. This concept has been the source of great debate, never more so than in the last two decades. The extremist understanding of jihad has by no means won the argument. There are almost 1.6 billion Muslims in the world. If every single Muslim believed that jihad was a violent struggle, the world would be a far more violent place.

The global monthly searches for 'jihad' and 'meaning of jihad' in Arabic are proportionally low, 4 per cent and 2 per cent of the number of searches for the corresponding English keywords respectively. This indicates that far more people in the English-speaking world are looking for information on the concept of jihad online than in the Arabic-speaking world. Further, the concentration of searches for these terms in Arabic tend to be in countries that are not involved in the jihad-inspired conflicts around the world today.

FIG. 4.3 Searches for 'Jihad' in the Arab World

Number of average monthly searches on Google



Algeria, Egypt, and Saudi Arabia are the countries with the highest number of average monthly searches for 'jihad' in Arabic. All three have been targets for jihadi violence in recent months. This does not necessarily mean there is not as much interest in the concept of jihad in the Arab world. It does point to the fact that some elements of jihadi ideology may resonate more, or less, in certain parts of the world. This information can, in turn, be used to construct more targeted counter-narratives.

THE ROLE OF THE INDIVIDUAL

Personalities have shaped the course of the global jihadi movement since its genesis. It is individuals who continue to be at the centre of shifts and developments in the movement today.

However, prominent jihadis online may not necessarily be those rousing the ranks on the world's battlefields. The most influential jihadis on the internet can be those who have provided the ideological justification for such violence to spread.

The Egyptian Sayyid Qutb, a highly influential Islamist who overhauled the Muslim Brotherhood's worldview to one more prone to violence during the 1950s and 1960s, is highly searched for in his native Egypt. But his name is also a popular search term in Saudi Arabia, where the religious and political landscape is very different indeed.

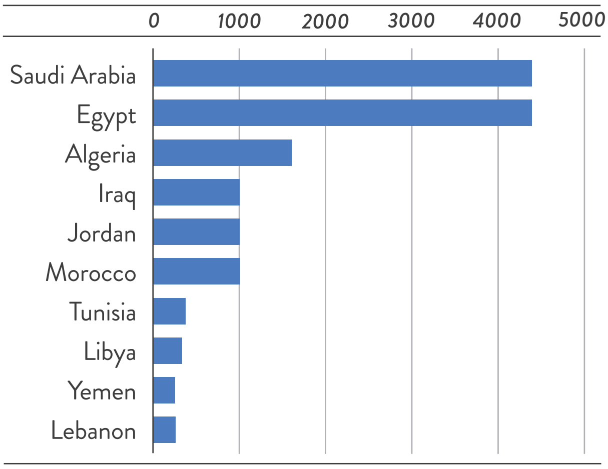
In both Egypt and Saudi Arabia, considered strong allies of the West in the fight against extremism and terrorism, there are almost 4,500 monthly searches for Qutb, who is credited with reviving the jihadi traditions of 13th century theologian Ibn Taymiyya. Qutb described the West and its supporters in the Muslim world as having reverted back to pre-Islamic *jahiliyyah*, or ignorance.

[40] "What is Jihadism," *BBC News*, 11 December, 2014, http://www.bbc.co.uk/news/world-middle-east-30411519.

[41] The five pillars of Islam are the five obligations that Muslims must strive to uphold in order to practice their faith. The five pillars are: the declaration of faith; ritual prayer; paying alms; fasting during Ramadan; and the Hajj pilgrimage.

FIG. 4.4 Searches for 'Sayyid Qutb' in the Arab World

Number of average monthly searches on Google

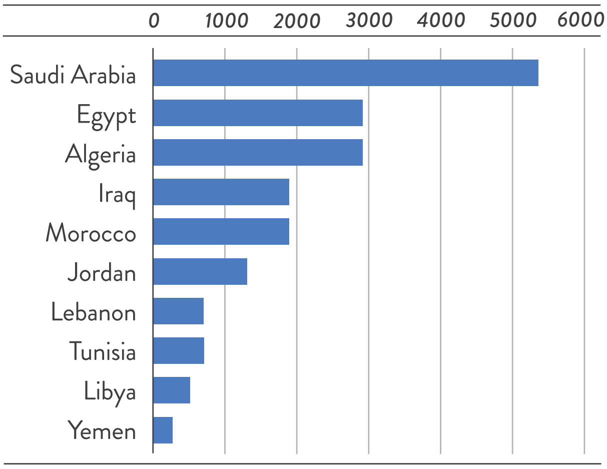


With the designation of *jahiliyyah*, Qutb sought to redefine the strategy and direction of the Muslim Brotherhood. He advocated for the abolition of jahili (ignorant) systems of governance using physical power and force if necessary.

The search frequency data for 'Sayyid Qutb' in Egypt and Saudi Arabia suggests there is an appetite for understanding more about him and his articulation of Islamic governance, which is starkly different to the systems in those countries. In Egypt, following the removal of the Muslim Brotherhood from power in July 2013, a court dissolved the group's political wing, the Freedom and Justice Party. The only Islamist party in the country's 2015 elections was the Salafi-oriented Nour Party. In Saudi Arabia, political participation from Islamist or any other type of group is not permitted.

FIG. 4.5 Searches for 'Ibn Taymiyya' in the Arab World

Number of average monthly searches on Google



Saudi Arabians search for 'Ibn Taymiyya' more than 5,000 times a month, far more than any other Arabic-speaking country. This is significant because jihadi groups today, such as ISIS and al-Qaeda, adhere with great rigour and literalism to the fatwas and dogma of radicals from Islamic history. Ibn Taymiyya occupies a particularly significant place among these.

It was Ibn Taymiyya who said that all Muslims must wage jihad against those who have been declared infidels, apostates, or even doubtful Muslims. It was also Ibn Taymiyya who gave legitimacy to the idea of treating civilians and non-combatants as 'collateral damage' when those waging violent jihad were conducting their attacks.[42]

But make no mistake, Ibn Taymiyya is by no means confined to the history books. Relatively modern jihadi manuals by the likes of Abdullah Azzam, Mohammad Abdul Salam Faraj, and Anwar al-Awlaki all draw heavily on the ideas of Ibn Taymiyya. Magazines circulated online today by ISIS and al-Qaeda also include excerpts from his works.

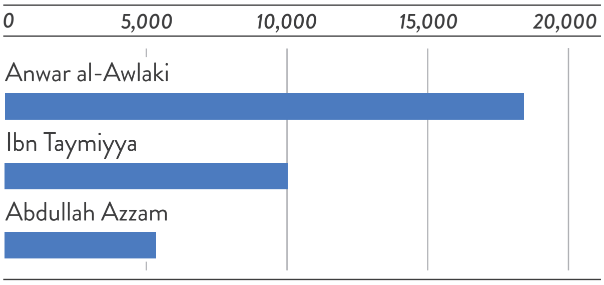
INFLUENTIAL ONLINE JIHADIS

Online, prominent jihadi personalities play a key role in disseminating jihadi ideology. A study by the Centre on Religion & Geopolitics (CRG) that looked at the lives of prominent jihadis found that key individuals, particularly ideologues, are crucial to keeping the jihadi movement alive.[43]

On the WorldofIslam.info website, books on a number of general religious topics, including jihad, are available. But alarmingly, these books include those written by key figures who have contributed to the development of the global jihadi movement.

FIG. 4.6 Global Searches for Leading Jihadi Personalities

Number of average monthly searches on Google



The first three books in the 'jihad' section are written by prominent individuals who have contributed significantly to jihadi thought. The first is Ibn Taymiyya, whose controversial Mardin fatwa has been the theological basis for jihadi groups targeting Muslims. The second is a 44-point guide from former al-Qaeda ideologue Anwar al-Awlaki on ways to support jihad. Abdullah Azzam's book, Defence of Mus-

[42] Shukur Khilkhal, "IS Emerges from Radical Islamic Jurisprudence," *Al-Monitor*, 12 August 2014, http://www.al-monitor.com/pulse/originals/2014/08/religious-origins-of-islamic-extremism.html

[43] Ahmed, Comerford, and El-Badawy, *Milestones to Militancy*.

lim Lands, also appears, along with a number of his other works on jihad. Azzam played a key role in the development of groups like al-Qaeda and Hamas, and is described as the 'father' of global jihad.

The search frequency analysis indicates there is much interest in these three, all of whom are dead. There are more internet searches for al-Awlaki, Ibn Tayymiyya and Azzam globally than for terms directly related to ISIS, including 'Caliphate ISIS' or 'Amaq Agency.'

Two of these three men were included in the sample of prominent jihadis used in the CRG study.[44] The third is often cited by jihadis when justifying acts of violence. In other words, there is no doubting their jihadi credentials. Some of these books have even resulted in convictions under the UK Terrorism Act 2000. Yet these seminal jihadi texts are hidden in plain sight on innocuous-looking websites alongside legitimate Islamic content. Technology firms need to understand which content is extremist, crosses a line, and warrants removal. Acquiring this knowledge and understanding which content should be of concern requires expertise.

THE CALIPHATE

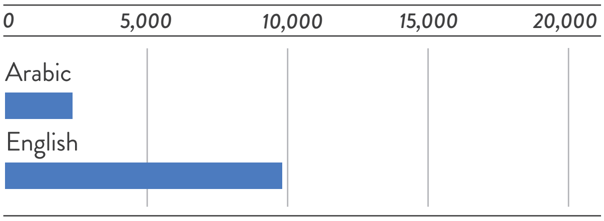
With the rise of ISIS and its proclamation of a 'caliphate' in parts of Syria and Iraq, the centuries-old Islamic system of governance has become one of the most talked-about phenomena in the history of Islamist extremism.

The online space in English and Arabic is different. Looking at global search frequencies for caliphate-related search terms gives us a valuable overview.

For both the search terms 'caliphate' and 'caliph' there is considerably more search activity in English than in Arabic, a similar trend to the keyword 'jihad.'

FIG. 4.7 Global searches for 'Khilafah' in Arabic and English

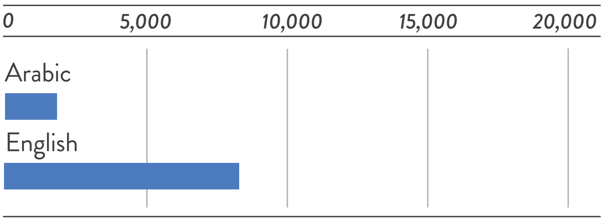
Number of average monthly searches on Google



As with the results for 'jihad,' this suggests more interest, or at least a greater knowledge gap, among English speakers when it comes to the idea of the 'caliphate.' The higher rate of searches in English might also indicate that the concept of a caliphate may not be as noteworthy for Arabic-speakers, compared to English-speakers.

FIG. 4.8 Global Searches for 'Khilafah' in Arabic and English

Number of average monthly searches on Google



REGIONAL KEYWORD ANALYSIS: UK/US

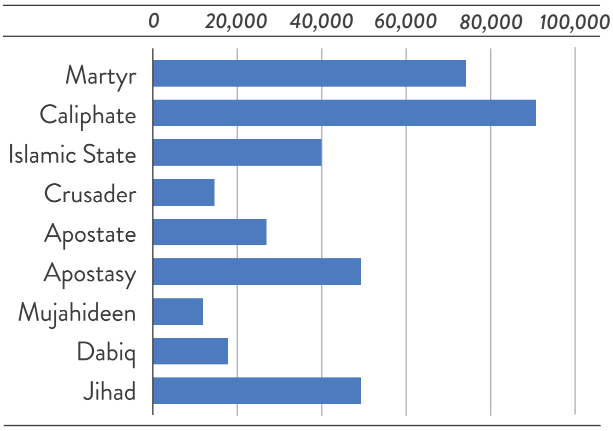
Keyword search frequency data can also be used to understand regional variations within the same country. For a whole host of reasons, including population, demographics, ethnicities, languages, poverty, and so on, there may be a noticeable difference in which keywords users search for.

We cannot track who is searching for what, but we are able to see whether a particular concept is being searched for more in certain places.

MONTHLY SEARCHES IN THE US

FIG. 4.9 Popular Searches in the US

Number of average monthly searches on Google



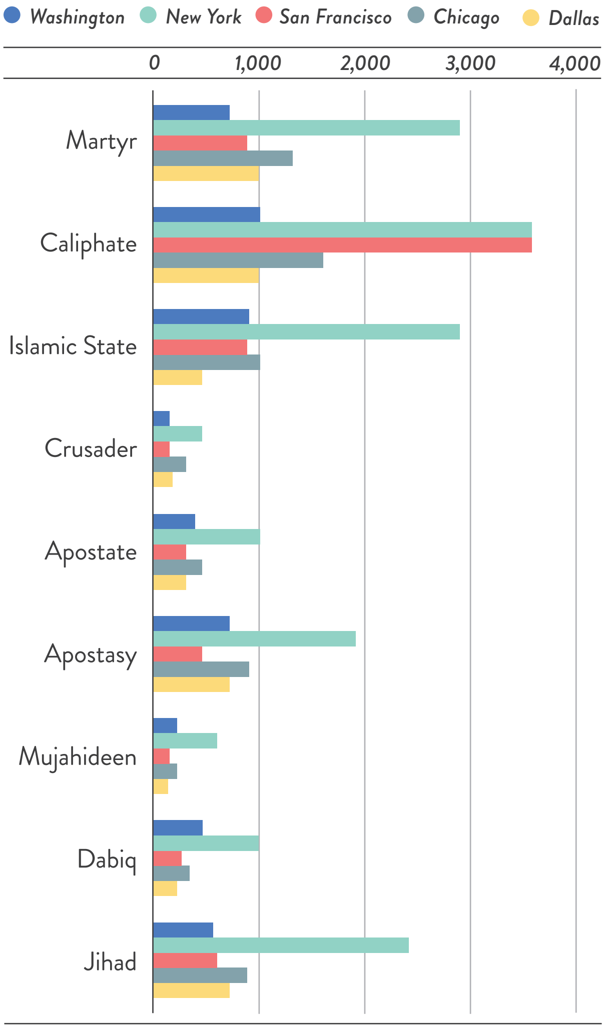
According to the data, there were an average of 49,500 monthly searches in the last 12 months for the keyword 'jihad' in the US, accounting for almost 30 per cent of global English searches for the word. Within the US, the greatest number of searches were in New York (2,400), while the average monthly searches in Chicago (880) and Dallas (720), were greater than those in Washington DC (590) and San Francisco (590).

The keyword 'Dabiq,' the name of ISIS' English-language propaganda magazine, has a global average monthly search frequency of 90,500, 20 per cent of which are in the US. Again, within the US, New York saw the highest number of searches (1,000), but that there were more searches on average in Washington DC (480) than there were in Chicago (320), San Francisco (260) and Dallas (210).

[44] Ibid, p.33.

FIG. 4.10 Popular Searches in the US

Number of average monthly searches on Google



Other trends we noticed were that, with the exception of New York, searches for 'martyr' (1,300) and 'caliphate' (1,600) were significantly higher in Chicago than in the other cities.

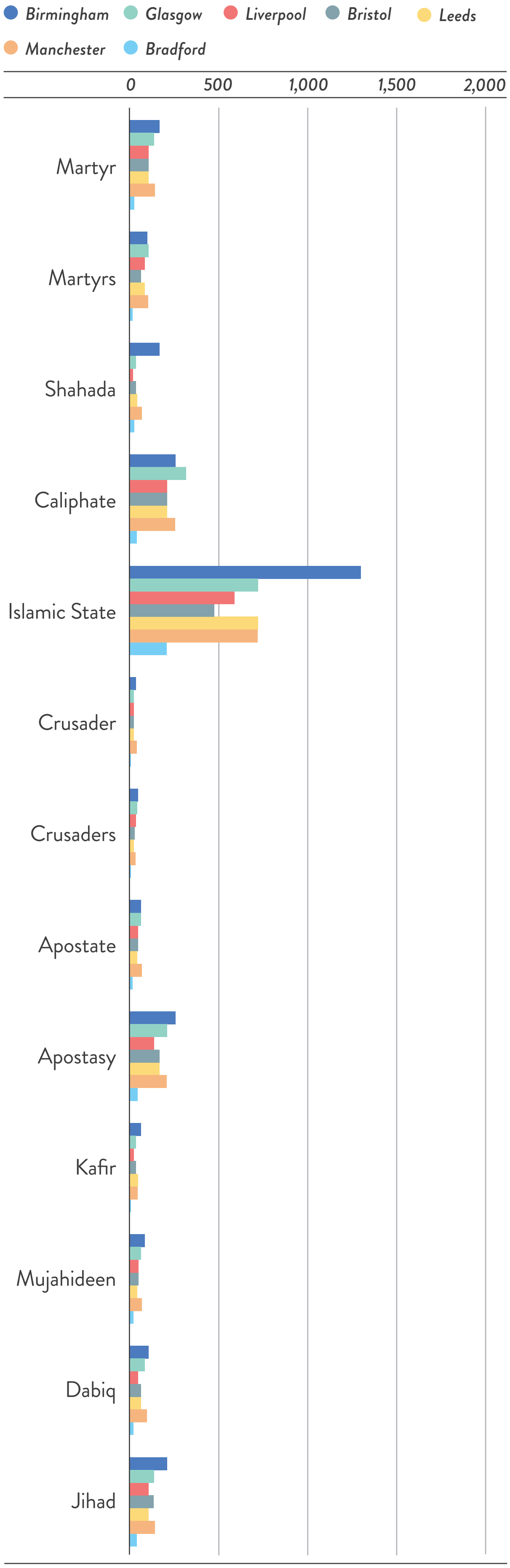
Washington DC, which is not only home to the US government and all its entities, but also to a host of research and policy organisations, has the lowest average monthly searches for 'crusader' (140) and 'martyr' (720), but ranks highly for 'Dabiq' (480) and 'caliphate' (1,000).

MONTHLY SEARCHES IN THE UK

The keywords with highest average monthly searches in the UK are 'Islamic State' (49,500), 'caliphate' (14,800), and 'apostasy' (14,800). During our research, just over 20 per cent of all the global searches for 'Islamic State' came from the UK, while the total number of US searches for the same term accounted for 17 per cent of global searches. This is striking given that the US has a far larger population than the UK.

FIG. 4.11 Popular Searches in the UK

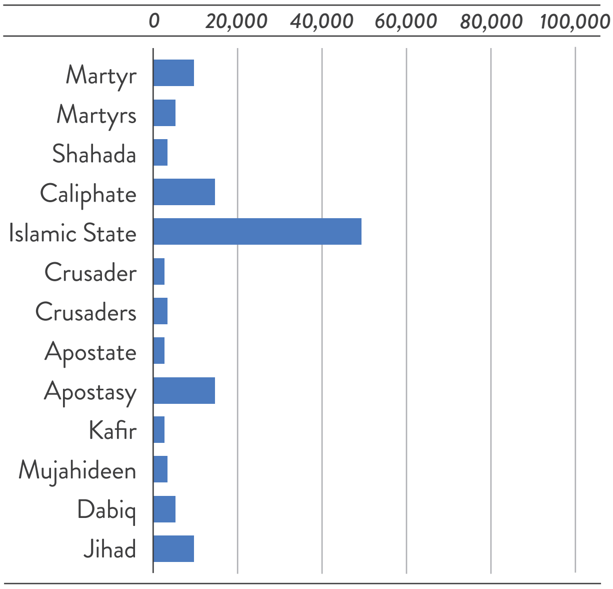
Number of average monthly searches on Google



Data from the searches for 'martyr' and 'martyrs' in Britain show the level of nuance needed to understand online trends and how best to counter them. While 'martyr' was searched 9,900 times, 'martyrs' was searched 5,400 times, a 4,500 difference. With a single letter, the search frequency almost doubled.

FIG. 4.12 Popular Searches in the UK

Number of average monthly searches on Google



We also looked at city-based search frequencies in the UK: in London, Manchester, Birmingham, Bradford, Leeds, Glasgow, and Bristol. While searches in London ranked significantly higher than the other cities, the others showed us what type of keywords users search for.

As with the US example, London, as both the UK's capital and most-populated city, dominated all of the frequency results. As such, in order to visualise the trends and be able to compare regional variations, London results have been omitted from the graph (see Figure 4.11).

Outside London, there were more searches for the keyword 'caliphate' in Glasgow (320) than there were in any other city in the sample, including Birmingham (260), which is the second-most populated British city.

There was a considerable gulf between the average monthly searches for 'Islamic State' in Birmingham (1,300) compared to any of the other cities. The number of searches for the same keyword was the same in Glasgow, Leeds, and Manchester, at 720 in each city, despite their different sizes.

WHAT DO WE DO WITH THIS DATA?

This data is a snapshot of the online landscape, one piece in an infinitely expanding and ever-changing jigsaw puzzle. But it provides information that can be used to make counter-extremism efforts more robust. It is only by bringing all of the major players in the online world together, with governments and civil society groups, that we can truly begin to battle the dominance of extremist content online.

By understanding that 'jihad' may be a highly searched for term in one country, or that the concept of the 'caliphate' may be searched for more in a certain city, counter-narrative providers gain a richer understanding of the threat. Taking the lessons from this breakdown and applying them on a global scale may reveal that particular strands of extremist ideology are more prevalent in certain places. This granular level of analysis would help target counter-narratives.

THE NEED TO SHARE DATA

This data is not intended to help snoop on groups belonging to a particular faith, or to curtail free speech. It is meant to help us understand the prevalent search trends so we can bolster efforts to counter extremism. The same approach should be adopted for addressing all forms of extremism, whether Islamophobic, anti-Semitic, homophobic, or racist.

By identifying trends and tendencies in particular regions, governments and civil society groups are better placed to run educational programmes to combat these ideas.

The above example is a snapshot of the wealth of data that could be harnessed to help challenge online extremism. However, the lack of cooperation between different technology companies, as well as with government and civil society groups, hampers progress.

Greater cooperation would help keep internet users safe. It would also help reduce the visibility of extremist ideas online in the long term. If extremist material is left unchallenged in the virtual world, it could manifest violently offline.

Major firms like Google, Facebook, and Twitter, despite their rivalry and competition, should consider sharing information with governments, civil society groups, and each other. In this online battle of ideas, there is a need to work together. Piecing together the analytics and trending information from various sources would help us better grasp the scale of the challenge. Most importantly, it would help identify opportunities to shift the online balance and protect vulnerable internet users.

PART FIVE

How Effective Are Counter-Narratives?

With extremist content readily available online, counter-narratives would help give users the full story. They are critical to broadcasting a moderate message, something severely lacking in prominence on the internet.

In our analysis, we categorised sites that came up in search engine results pages (SERPs) as having extreme, counter-narrative, or neutral content. The term neutral referred to the effect material might have on an average internet user. This breakdown allowed Centre on Religion & Geopolitics (CRG) and Digitalis to understand how balanced the SERPs for certain search terms were, and what content type they were weighted towards.

Of the 47 SERPs we analysed for balance, only five were weighted towards counter-narratives.[45] In fact, we only found such narratives in 10 of the SERPs we analysed. A very small proportion of sites we looked at contained counter-narratives, 43 out of a total of 870.

THE NEED FOR A VOICE

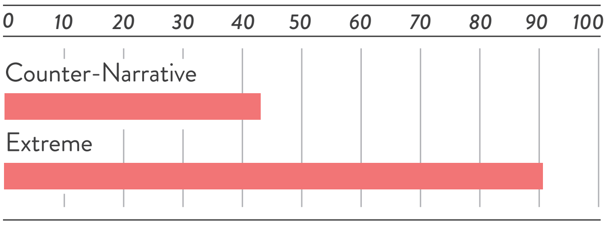
Counter-narratives need to appear alongside extremist content online to provide balance, if not to drown it out completely. However, counter-narratives only competed directly with extreme content in eight cases.

When analysing the first two pages of the SERP for the 47 keyword sample, the lack of a counter-narrative voice was apparent. We documented extremist content in 28 of the SERPs, 19 of which were uncontested by counter-narrative content. In light of this data, it is clear that counter-narratives are simply not competing regularly enough. Further, in the eight instances where there was direct competition, the balance of the first two pages of the SERPs were only weighted towards counter-narratives on two occasions.

Counter-narratives currently do not have a loud enough voice online. The balance in the SERPs is weighted towards extremist messages. But more importantly, the extremist voice is being heard in the first two pages of the search engine results, which are the most prominent and viewed, thus the most important areas of the SERP. Counter-narratives, meanwhile, are performing poorly in this respect.

FIG. 5.1 Extreme and Counter-Narrative Content Found

Total number found



Overall, we founda that counter-narratives lack cohesion, purpose, and a nuanced understanding of the online world. We classified counter-narrative content according to three categories – civil society, government, and religious organisations. We only looked at the organic area of the SERP; 'pay-per-click' adverts were omitted for the purpose of this study.

Of the 43 counter-narratives identified, visibly Muslim-led efforts were the most common, with 39 recognised. Only one counter-narrative was identified as being government-backed, a tiny proportion of the 870 sites we discovered in this SERP analysis.

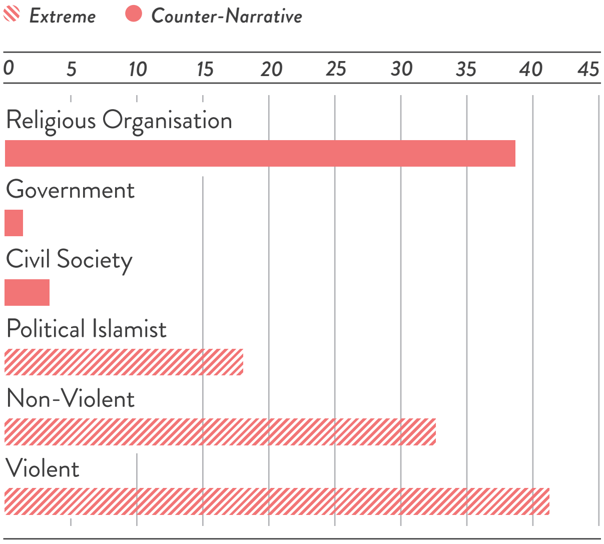
While our research identified a variety of extremist content in SERPs, that variety was absent in counter-narrative efforts, where Muslim-led initiatives dominated. This suggests that counter-narrative initiatives led by governments and civil society groups are under-resourced and not achieving sufficient natural interest. It also implies that they are not joining forces to bolster their online presence. Instead, a melee of groups are trying to address the balance on their own. Working together, with a thought-out strategy, they may be able to challenge extremist content with counter-narratives more directly.

The linking data also points to this lack of cohesion in counter-efforts. Whereas extremist content was found to link

[45] For a partial list of keywords see Appendix.

FIG. 5.2 Categories of Content Found

Total number of pages found



well with big sites such as Kalamullah.com, Ummah.com, and IslamQA.info, counter-narratives did not have similar relationships with major sites. As a result, their online presence could be considered weak. Such a relationship between several sites would help promote counter-narratives and enable them to rank higher in target SERPs.

The counter-narratives we believe should be actively promoted and supported, owing to the suitability of their content and message, were analysed for the links entering into them. It became clear that they were hopelessly inadequate and could not compete with extremist content. Furthermore, a set of relatively recent online counter-narrative efforts that were identified as having good quality content did not appear a single time during the SERP analysis for any of the 47 keywords that were analysed.

The leading Muslim counter-narrative sites that have appeared in recent years also lack the online presence needed to challenge extremist material. Sandala.org, the official website of internationally renowned Islamic scholar Hamza Yusuf, who served as an advisor on Islam to former US President George W. Bush; Perrenialvision.org, which seeks to bring together Muslim voices to address the most pressing issues facing Muslims today; and Haqiqah.org, a moderate response to ISIS' *Dabiq* magazine are examples of high quality counter-narrative sites that lack online presence. While Sandala.org has 25,503 links coming into its site, Perennialvision.org has just seven, and Haqiqah.org has 110. This should be a wake-up call: Producing good content is not enough. It must be optimised to challenge the SERPs that are dominated by extremism. Counter-narrative initiatives must acknowledge the need for search engine optimisation (SEO), and harness its power to promote their crucial message online.

Even government-supported counter-narrative sites are yet to match up fully. Linking data for the UK government's Research, Information & Communications Unit (RICU) page showed only four links entering into it, with the site as a whole receiving 2,617 links. The site containing the British government's *Counter-Extremism Strategy* only returned 634 links entering into it. Partly as a result of insufficient linking, these efforts do not appear in the organic areas of search engine results pages. Therefore, they do not challenge in the same space as extremist content.

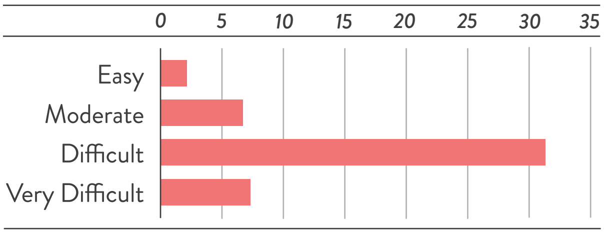
By comparison, sites we identified as hosting extremist content have far stronger linking data and, partly as a result of this, they featured prominently in the SERPs. Khilafah.com has 103,567 links, Kalamullah.com has 378,169, and Ummah.com has 98,410.

Meanwhile, counter-narratives that came up in the SERPs were sometimes dated or unappealing compared to extremist content. Although these sites were set up in order to fight this online battle of ideas, they cannot compete against slick sites carrying extremist messages. The counter-narrative sites we found in the SERPs had large bodies of detailed text, old-fashioned graphics, and often a confusing message. This is clearly not going to engage young, savvy internet users.

Much of the information gathering by users that we observed in our research occurred via 'Q&A' websites like Ummah.com, an open forum for Islamic discussions, and IslamQA.info, a closed-format fatwa-issuing website. Both sites are vehicles for religious dialogue. On these forums, questions on moderate issues are often hijacked in the comments sections by people expressing extremist messages, with no counter-message to balance those views. Forums at the very least must be properly moderated, with flagging options and warning messages included so users can prevent extremists hijacking the thread. This is by no means a call for censorship, but counter-narratives need to be able to present their message.

FIG. 5.3 How Easy is it to Introduce New Content into the SERPs?

By percentage of SERPs analysed [46]



Further, today's most up-to-date counter-narrative sites only offer users a passive experience. Videos, lectures, or pages with dense prose explain what we should think. Investment in a well-moderated, interactive site that facili-

[46] For more on the difficulty of introducing new content to the SERP, see 'Identifying the Possibilities,' p.51 of this report.

tates ideological debate would help shift the balance of ideas online. It would also compete directly with websites using the same format to promote extremist views.

To effectively tackle the impact of websites spreading extremist content online, two areas must be addressed. First, we need robust counter-narrative sites that keep up with sites featuring extremist material. Second, we must ensure they are optimised to challenge extremism in the right spaces.

Finally, a counter-narrative campaign should engage pre-emptively in the online debate. This is where agility is vital to success. Monitoring trends online, in relation to target keywords and their SERPs, would allow alternative narratives to target strategic areas of concern, before these areas become even more tainted with extremist content.

This study has already identified areas of focus. SERP analysis identified 16 keywords, with an accumulated search frequency per month of 708,600 globally and 83,510 in the UK, which contained no extremist or counter-narrative content in the SERPs. We should seize this opportunity for online counter-narratives to move from reactive tactics to a pro-active operation.

However, in order to engage in this process, the counter-narrative offering needs improvement. The majority of these alternatives do not compete quite simply because there are too few of them, and they lack strength in presence and messaging.

CASE STUDY

Counter-Narrative Examples

Two notable efforts to present a moderate Islamic voice online are PerrenialVision.org and Haqiqah.org. Both websites are well-designed, have appropriate content, and are easy to navigate, however they did not appear in a single SERP during our analysis of keywords. This exemplifies the nature of the problem; it is not just about an absence of counter-narratives, but the lack of sophistication in technical optimisation that would enable these websites to challenge extremist content in search results.

Conversely, this study found that the Muslim-led counter-messaging sites that did feature prominently in the SERP were dated and visually unappealing. Nevertheless, these efforts present moderate ideas in the areas where they are most needed. The top result for the keyword 'jihad' is an explainer by the Islamic Supreme Council of America, which addresses the misunderstandings around the concept. Similarly, the website Aboutjihad.com presents a more balanced understanding of the concept of jihad. It ranks prominently in the SERP for 'jihad' and related searches, but it is by no means a modern, user-friendly website.

Successful counter-narratives online must be sufficiently optimised to challenge extremist content online.

MUSLIM EFFORTS DOMINATE COUNTER-NARRATIVES

The first stage of categorising the SERP results for the 47 selected keywords was to identify whether the searches were dominated by extremist content or counter-narratives. The next stage of SERP analysis involved categorising each of the identified extremist or counter-narrative websites by type.

The extremist content was categorised into violent, non-violent extreme content, and political Islamist content. Similarly, the counter-narrative websites were divided into those backed by governments, civil society groups, or Muslim groups.

By breaking down the source of each counter-narrative initiative identified in our analysis, the research found counter-narratives were dominated by Muslim-led sites. While some accuse Muslims of not doing enough to grapple with religious extremism, these findings suggest Muslims are at the very forefront of this online battle.

The poisonous extremist ideology that has hijacked Islam relies on relaying a distorted and politicised version of the faith. Muslims around the world, with help from us all, must lead the fight against this ideology because they are best equipped to do so. While the data shows Muslim-led efforts are dominating in this area, they are still not adequately contesting extremist content. They are in need of support from governments and technology companies if their efforts are to be truly effective.

It is not enough, and it is not productive, to simply support the actions of building and hosting websites, or to provide space for targeted advertising. The nature of the internet and the habits of internet users today mean that counter-narrative websites need a high degree of technological expertise to ensure their content can mount a challenge to, if not dominate, extremist content in SERPs.

PART SIX

How Can We Secure the Online Space?

The study has clearly found that extremist material is readily accessible online in many different forms through a variety of keywords, and that anyone could chance upon it while browsing the internet. If we allow sites providing extremist content to self-promote through acquisition of links and content addition with no competition from counter-narratives, extremist messages will continue to dominate online. Google's enormous market share in internet search has made it the de-facto online content control marshal, with governments required to take a back seat.

This is despite the British government, in its 2011 *Prevent Strategy*, acknowledging that one of the measures required to curb the threat of radicalisation online is the need "to limit access to harmful content online in specific sectors... and ensure that action is taken to try to remove unlawful and harmful content from the internet." However, as David Cameron's foreword in the 2015 *Countering Extremism Strategy* says, this is "not something the state can do alone. [It] needs the help of everyone."

The online battle for ideas may seem like a new phenomenon, but we can always learn lessons from the past. An insurgency is defined as a rebellion and an effort to overthrow the government. In many respects, the threat posed by extremism online, whether on social media or other websites, is a type of insurgency, in which extremists actively engage in efforts to spread their ideas and exploit the online terrain.

In 2006, US General (then Lieutenant General) David Petraeus and General (then Lieutenant General) James Amos, made a very brave decision. They accepted that there were doctrinal and tactical failings in the armed forces' attitude towards the insurgencies rising out of the power vacuums left by regime changes in Iraq and Afghanistan. They were losing the battle of ideas.

In December 2006 the *Counterinsurgency Field Manual*[47] was issued to soldiers, the first to be released in the US Army for 20 years and for 25 years in the US Marine Corps. Based on this doctrine, the British Army released its own *Counterinsurgency Field Manual* in October 2009.[48] The British Army's manual contained a set of 10 principles that looked to educate troops on how to combat an insurgency.

Fighting extremism is a "battle of ideas" as stated by the former British Prime Minister,[49] and extremist ideas are quickly filling a gap in the online landscape. Although the principles outlined below were designed for fighting insurgencies, they resonate with the challenge we face on the internet today. Governments must take a step back, admit tactical defeat, and implement sustainable policies to ensure real change.

STRATEGIES OF COUNTER-INSURGENCY AND THEIR APPLICATION ONLINE

1 Primacy of Political Purpose

"Active political involvement is required in order to guide how a campaign develops."[50] Currently, no government has taken a strong enough lead on countering extremism online. Without this political purpose, any online work will lack legitimacy and be void of long-term stability.

2 Unity of Effort

"An insurgency can only be defeated if the host government, a coalition or alliance, and their many instruments of state work together towards a common end."[51] Today, we have all the information we need to tackle online extremism,

[47] *The US Army – Marine Corps Counterinsurgency Field Manual*, University of Chicago Press, Chicago: December 2006.

[48] Ministry of Defence, *British Army Field Manual Volume 1, Part 10 - Countering Insurgency*, Army Code 71876 (London: October 2009), https://www.scribd.com/document/28411813/British-Army-Field-Manual-Counterinsurgency-2009.

[49] David Cameron, "Extremism: PM Speech" (speech, Birmingham, 20 July, 2015), https://www.gov.uk/government/speeches/extremism-pm-speech.

[50] Ministry of Defence, *British Army Field Manual Volume 1, Part 10*.

[51] Ibid.

but it is dispersed among technology companies, internet providers, governments, civil society groups, and religious organisations. They rarely share it. Current policy lacks the unified action and information sharing required for counter-efforts to succeed.

3 Understand the Human Terrain

“This is a broad and complex subject which brings together sociology, political science, geography, regional studies, linguistics, and intelligence.”[52] The online terrain is similarly complex, and arguably more so. Only with expertise in several different fields, including from government, technology companies, academia, civil society, and religious organisations, will policy begin to bring order to a chaotic virtual universe.

4 Secure the Population

“The principle focus… must be the security of the population.”[53] It is not enough to attack extremism on social media, leaving online users open to extremism in the search engine results pages. The search results must be won, before the strongholds of social media are attempted. There is also a need to develop critical-thinking skills, particularly among young people, in order to equip users to navigate the internet more safely.

5 Neutralise the Insurgent

“The insurgent can be neutralised by a blend of physical and psychological means.”[54] Extremists online must be given no room for manoeuvre. Progress on the peripheries can be started immediately. We can look to fill the information vacuum online, eventually making it very difficult to find extremist information channels, unless a user is purposefully searching for them.

6 Gain and Maintain Popular Support

“It gives authority to the campaign and helps establish legitimacy.”[55] In order to maintain legitimacy, it is vital that this does not become a censorship campaign. Popular support will be lost if filtering is the dominant method of countering extremism. Monitoring and providing a balanced narrative through positive measures will gain and maintain the support of media outlets, moderate religious organisations, and the public at large.

7 Operate in Accordance with the Law

“It is always counterproductive for security forces to operate outside of the law.”[56] Although this seems obvious, it is vital to continue operating with the concept of a ‘free internet’ in mind and to uphold laws governing this space.

8 Integrate Intelligence

“Information is more important than firepower.”[57] Governments and regulatory bodies can expend hours of manpower pursuing extremism online and having it removed, only to find that three or four new items or sites have replaced it. With open lines of communication between policy makers, and those with detailed analytics information, much extremist material can be kept out of the first pages of the search engine results pages (SERPs).

9 Prepare for the Long Term

“Preparing for the long term through the campaign plan is the means by which effective integration of cross-government effort can be maintained.”[58] The trends that lead extremism will be different in the long term. We should identify the ideological causes of extremism in order to allow efforts to be relevant in the future.

10 Learn and Adapt

“Forces must quickly and continually adapt conventional capabilities and approaches.”[59] The ever-evolving landscape of the internet changes at such a pace that analysis must be continuous and sustained so that we have an accurate understanding of the online environment. Constant monitoring and agility is required to effectively combat extremism on the internet.

CURRENT CONTENT CONTROL

While Google, as well as other major technology firms, are acutely aware of the danger posed by extremist content online, these companies, understandably, do not want to be perceived as policing the internet. Also, due to the complexity surrounding their algorithm, Google is not able to alter SERPs at every request and does not have the capacity to monitor all the information introduced into their index. This has clearly created blind spots, as evidenced by the huge amount of readily available extremist content discovered by the Centre on Religion & Geopolitics (CRG) and Digitalis. A unified effort on the part of governments, Google, and supporting third parties with cyber and technological knowl-

[52] Ibid, p.41.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

edge, is required to introduce and promote counter-narrative content that can effectively challenge extremist content in the SERPs.

The government, in its 2011 *Prevent Strategy*, described the need "to limit access to harmful content online... and ensure that action is taken to try to remove unlawful and harmful content" as one of the core measures required to curb the threat of radicalisation online.[60] However, the former Prime Minister's foreword in the 2015 *Counter-Extremism Strategy* demonstrates it is "not something the state can do alone. [It] need[s] the help of everyone."[61]

While Google and other technology companies respond well to individual and specific requests for removal, a unified effort combining governments, leading internet firms and supporting third parties will be required to not only introduce, but also to successfully promote, counter-narratives. This challenge is best demonstrated where extremist content resides unexpectedly on non-extremist and otherwise legitimate sites to which third parties have unrestricted access.

CASE STUDY

Google, Censorship & Content Control

The concept of de-prioritising or de-listing specific websites, indeed whole areas of subject matter, is not new to search engines. Baidu, a Chinese web services firm, is heavily controlled and, while Google pulled out of that market, it adhered to the country's strict censorship rules until 2010. In fact, Google is increasingly accustomed to the geopolitical nuances of particular territories. The company bowed to legislative pressure in Turkey, Russia, and elsewhere.

In civil libel and privacy applications, the search giant's starting modus operandi is always that its algorithm is automated, and its server farm structure so vast that intervention is at least difficult, and almost certainly disproportionate. But in other areas, major controls have been implemented, whether unilaterally or under the weight of government intervention.

Essentially there are two ways in which a search engine might censor content:

- Delisting entire sites or pages either for the results for specific search phrases or entirely from search engine results pages (SERPs) (this is often done manually, as a result of a legitimate application).
- Making changes to its search algorithm to ensure specific types of content are automatically 'de-prioritised' or indeed delisted, thus featuring lower generally in SERPs for any search phrase.

Automated Intervention

- In Germany and France, Google has removed white supremacist, Nazi, anti-Semitic, and other websites in order to comply with local laws.[62] It also blocks (automatically) some terms from its autocomplete function in the search bar such as hate or violence-related keywords, pornographic terms, and other legally-mandated removals.
- In 2012, Google Shopping policies were modified to prohibit the inclusion of firearms and firearm-related products, such as ammunition and accessory kits.[63]
- And while not wanting to be considered a monitoring entity, Google clearly does have certain automated algorithmic indicators which remove sites, such as those which have been hacked for the purposes of spam (often in the pharmaceuticals and gambling industries).
- The 'Mugshot Algorithm' change: so frequently were police mugshots of people arrested but not charged featuring in its image results, that Google implemented an algorithmic change to remedy the situation.[64]

Manual Intervention

- In piracy, Google announced in 2012 that it would 'down-rank' sites where multiple valid applications had been made for it to do so. But in 2014 it went further, promising to "tweak its search engine" and to refine the relevant "signal," a clear sign of something more automated being deployed.[65] The company's report later on its blog suggested again that the approach is more about removing specific pages following human notifi-

[60] HM Government, *Prevent Strategy*.

[61] HM Government, *Counter-Extremism Strategy*, London: October 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf.

[62] Jonathan Zittrain and Benjamin Edelman, "Localised Google Search Result Exclusions: Statement of Issues and Call for Data," Berkman Center for Internet & Society: Harvard Law School, October 22, 2002, https://cyber.law.harvard.edu/filtering/google/.

[63] Nick Leghorn, "Google to Censor Firearms Related Shopping Results," *The Truth About Guns*, June 28, 2012, http://www.thetruthaboutguns.com/2012/06/foghorn/google-censor-firearms-related-shopping-results/.

[64] Barry Schwartz, "Google Launches Fix to Stop Mugshot Sites from Ranking: Google's MugShot Algorithm," *Search Engine Land*, 7 October, 2013, http://searchengineland.com/google-launches-fix-to-stop-mugshot-sites-from-ranking-googles-mugshot-algorithm-173672

[65] Stuart Dredge, "Google Says Latest Search Changes Will 'Visibly Affect' Piracy Site Rankings," *The Guardian*, 20 October, 2014, https://www.theguardian.com/technology/2014/oct/20/google-search-changes-piracy-rankings.

cation.[66] In its Transparency Report Google suggests it is dealing with applications for removal of some 24 million copyright-infringing webpages per week. The firm claims it responds within six hours on average. [67]

- The ‘Right to be Forgotten’ judgment against Google in Europe obliged the company to remove outdated and erroneous information from an individual’s search engine results upon request, with some exceptions. Google has created an entire team to validate and vet such enquiries, and since May 2014 it has removed 43 per cent of URLS evaluated, equating to more than 500,000 removals.

It is safe to say that, should it wish or if it were legislated into doing so, Google and other search engines can mitigate the audience of a particular piece of content or, generically, a type of content. It is the view of the authors of this report that tech giants are relatively advanced in their efforts to respond (manually) to legitimate removal requests. The challenge in combatting extremist content is that there is so much of it and it can be so tricky to identify. It would be wrong to expect Silicon Valley to fix the matter alone.

The added challenge of extremist, sometimes illegal, content on individual pages, within otherwise legitimate sites, further compounds the issue. The potential deliberate promotion of this content using the authority of legitimate websites as collateral does too.

Given the subjective challenge and inevitable difficulty for any automated algorithmic calculation to identify all violent extremist content and understand which components of specific sites might (and those which might not) be rightly targeted, this report does not advocate policy that places the entire burden of doing so on search engines like Google.

CASE STUDY

Pay-Per-Click Advertising on Search Engines

Pay-per-Click (PPC) is the method through which advertisements are sold on most search engines. It has become a universal tool in a marketer’s armoury. Google’s AdWords PPC platform continues to make up the lion’s share of the search giant’s global revenue.

How it Works

PPC allows one’s advert to appear when a user in a specified geographic territory searches on a particular keyword or phrase. Many people might see a PPC advert having searched for the phrase in question, but an advertiser will only pay (at a pre-agreed ‘cost-per-click’) for the proportion of searchers (typically around three per cent) who actually click on the link and land on the advertiser’s website.

Its Value

Unsurprisingly, PPC has become an essential part of most brands’ online customer acquisition strategy, partly because it is so highly-targeted and partly because its effect is completely transparent. Users can be tracked through a site after clicking on an advert so that, for instance, a shoe retailer knows exactly how many people who searched for ‘brogues,’ end up buying them, how much they spent and, of course, the resultant return on investment.

How it Appears

PPC adverts feature at the top and/or bottom of the results page. Despite Google having made those results look increasingly more like the ‘organic’ (non-paid) search results, consumers typically recognise them as adverts and they tend to reap (in aggregate) only around 30 per cent of the traffic from a SERP.

PPC’s Role in Countering Extremism

In the online battle for share of voice in sensitive areas of debate, the case for PPC is weaker for the following reasons:

1 Traffic share is typically minimal. While ten PPC advertisers fighting for their respective three per cent of retail traffic around a specific product phrase may reap significant revenue, the same share of voice does little to rebalance debate in an otherwise unbalanced page of results.

2 Trust is low. Consumers increasingly recognise PPC as paid advertising. When one is looking for a product this can be perfectly aligned with one’s needs, but when seeking answers to questions, a paid advert by a government entity, or other group, may be less compelling and seem less objective.

It was widely reported that BP at the height of the Deepwater Horizon oil spill in the Gulf of Mexico in 2010, spent one million pounds a month on trying to achieve share of voice in the face of much adverse criticism.[68] Budget deployed on PPC stood out as being sponsored content and

[66] Fred von Lohmann,“Report: How Google Fights Piracy,” *Google Public Policy Blog*, 10 September, 2013, https://publicpolicy.googleblog.com/2013/09/report-how-google-fights-piracy.html.

[67] *Google Transparency Report*, Google, https://www.google.com/transparencyreport/removals/copyright/?hl=en.

[68] Mohamed Mejri and Daniel De Wolf, “Crisis Management:Lessons Learnt from the BP Deepwater Horizon Spill Oil,” *Business Management and Strategy Journal* 4, no.2 (2013), https://orbi.ulg.ac.be/bitstream/2268/165986/1/Crisis%20Management-%20BMS.pdf.

would have achieved around three per cent share of voice. In contrast, successful ranking in the organic listings achieve an aggregate 70 per cent of traffic, the first ranked listing alone typically commanding over 30 per cent.

ADDRESSING THE BALANCE

Online counter-narratives need greater agility in order to engage in the debate and present a much-needed balanced voice. A focused counter-narrative campaign should be broken down into three stages: monitoring and understanding; achieving impact; and recognising new areas for the introduction of narratives.

This study has demonstrated what the monitoring and targeting stage should look like. Using the knowledge and expertise of several parties, new light can be shed on the online status quo. Recommendations can then be combined with knowledge of ideology and current trends, including analytics data, to gain a greater understanding of what is needed.

Once the requirements are identified, content could be created (where necessary), introduced, and promoted in the target SERPs. To demonstrate this, Digitalis completed impact analysis on the SERPs of the 47 keyword sample. Impact analysis uses technology to identify the ease of introducing counter-narratives into the SERPs of target keywords. The results were varied, and suggested that, in most cases, introducing content would need to be a sustained project, with quick wins available in the short term.

STRATEGIES

Various strategies and campaigns could be implemented, depending on the issues discovered online. Below is an outline of a best and worst-case scenario. The best-case scenario offers one possible solution that could act as a guide for other potential future online counter-extremism campaigns and is designed to shine a light on what is required by all stakeholders. This should therefore not be considered as the solution, but a solution to the problem areas our research identified. The worst case offers a suggestion of what could occur if no action is taken.

BEST CASE SCENARIO

In the best-case scenario, search engines and social media companies would work in unison with technology companies and governments to tackle online extremism. The ability to directly impact SERPs, either by removing specific web pages from the search engine data storage, referred to as an index, or altering a search engine algorithm to penalise how a certain site or URL ranks, would support promotion work.

An active campaign site to counter all identified extremist content could be created, promoted through the backing of mainstream media and multiple governments. A core, government-backed platform would facilitate the creation of satellite websites and supporting social platforms, which would help with the variety of content needed to rank highly in the various target SERPs.

Noticeable effects could be achieved in a short space of time once a campaign has been launched and the end goal would be reaching a saturation point with counter-narratives, where extremist content would be outranked in the results pages.

WORST CASE SCENARIO

In the worst case, efforts by individual organisations would continue with no unified purpose. As no single organisation has the resources to create or maintain the extensive network of sites and satellite sites required to challenge extremism online, the effect would not be strong enough.

Other tasks such as monitoring and analysing online trends require further time and expertise. Without a unified front to fight online extremism it is unlikely coverage for counter-narratives on the major keywords of concern could not be achieved. In this scenario, the work would lack the agility and pre-emptive tactics to target the key online spaces. Extremist content would continue to be prevalent in unmonitored SERPs. The online battle would go on.

Methodology

Utilising its experience and extensive background knowledge, the Centre on Religion & Geopolitics (CRG) constructed a list of keywords that could potentially lead users to extremist content, whether intentionally or otherwise, if entered into a search engine. These keywords were categorised based on their ideological type and potential risk associated with them (see Keyword Categorisation). For each of these keywords, Digitalis ascertained the average number of times it is searched in Google per month, both globally and within specific regions. CRG also compiled a list of a small number of websites, known, or suspected to be of concern, in regard to extremist content. Digitalis collected the linking data for each of these websites and subsequently for any further websites of interest discovered either on examination of said linking data or during the the search engine results pages (SERP) analysis.

From the total list of keywords constructed by CRG, two samples were selected for further analysis. The first sample consisted of those keywords that are searched most often. The second sample consisted of keywords considered to pose a high risk of association with extremism. Each of these keywords was entered into Google and the content ranking within the first two pages of the resultant search listings was analysed. Each item of content found within the results was categorised as extreme, counter-narrative, or neutral. Following the categorisation of each item of content discovered, it was possible to determine the ratio of extreme content to counter-narrative content within the first two pages of results for each category of keyword search.

Beyond the categorisation of content, further technical analysis was carried out on the results for the keyword searches in order to determine the strength of the SERPs and the ease with which new content could permeate the most prominent ranking positions.

THE INITIAL INFORMATION SEARCH

In compiling the list of keywords to analyse, CRG considered a breadth of words and phrases that might be used in general research on Islam and also those that might be used in deliberate attempts to access extremist content. This list was used as a basis to ascertain further potential associated keywords through the use of tools such as the Google Keyword Planner, as well as examination of Google Suggest phrases and Google-related searches. The final list of 287 keywords comprised 143 English keywords and 144 corresponding Arabic translations.[69]

KEYWORD CATEGORISATION

In order to identify the nature of each type of enquiry, the keywords were allocated to one of four categories:

- Category 1: extreme, violent keyword
- Category 2: extreme, non-violent keyword
- Category 3: Islamist, non-violent keyword
- Category 4: moderate, general keyword

The categorisation of the keywords was designed to indicate the differing nature of the various keyword enquiries; some keywords, such as 'beheading' or 'killing apostates' are inherently violent, whereas others, such as 'crusades' or 'caliphate' are more general in their nature and, as such, would be expected to generate a different type of content.

Extreme, Violent	Extreme, Non-Violent	Islamist, Non-Violent	Moderate, General
Suicide Vest	*Dabiq*	*Khilafah*	Martyr
Killing Apostates	*Kafir*	*Khalifah*	Jihad
How to do Jihad	*Rafida*	Meaning of *Khilafah*	*Shahada*

These categories are by no means definitive, but served to broadly categorise the keywords in order to better understand how different keywords, some ostensibly more extreme than others, return extremist content in the SERP. Given that extremist ideologies draw on the same religious values and thoughts as held by mainstream Muslims, there was a need to grade each keyword in order to reflect the level of risk associated with each keyword.

[69] For a partial list of keywords see Appendix.

It is inevitable that there is some degree of overlap between the categories, however the designation reflects the nature of the keyword itself, rather than its connotations with any particular group. This meant that while the concept of 'khilafah' (caliphate) is most associated with ISIS, the word itself does not have any inherently violent or extreme connotations. As a result it was categorised more reflectively in the political Islamist keyword list.

In a general sense, keywords that were categorised into the extreme violent and extreme non-violent were those that were more institutionalised and closely associated with the rhetoric of known jihadi groups like ISIS and al-Qaeda, with the keywords in the other categories reflecting a more general, non-institutional nature.

KEYWORD FREQUENCIES

To gain an understanding of the popularity of the keywords on the list, Digitalis ran the selected keywords through Google Keyword Planner, which uses historical data to provide an average monthly search frequency for each keyword, which can be filtered to a chosen geographic region.

The frequencies in the study are monthly averages taking into account Google's historical data from the past 12 months (April 2015 – April 2016) and only relate to searches made using the Google search engine.

As the study did not have access to Google's comprehensive data, these average frequencies can be used as a useful guide to keyword popularity and geographic trends, but do not give exact or conclusive figures.
Initially, the keywords were analysed for their global search frequencies. It was then decided to analyse the effect that geographic breakdown in the United Kingdom, United States, and Arab countries would have on the average monthly search frequencies.

Cities in the UK and US were chosen through a combination of size and geographic spread relevant to the country. The idea here was to gain the widest cross-section for a significant number of the population. Specific city data was not available for the entirety of the Arab world, so for completeness it was decided to focus on whole countries.

Global frequencies were gathered for both English and Arabic keywords. However only English keywords were used for the UK and US, and only the Arabic translations were used for the Arabic-speaking world.

The following geographic filters were used:

United Kingdom	London Birmingham Leeds Glasgow Liverpool Bristol Leeds Manchester Bradford
United States	Washington DC New York (city) San Francisco Chicago Dallas Montgomery
Arabic-Speaking World	Iraq Saudi Arabia Yemen Jordan Lebanon Israel Egypt Morocco Libya Algeria Tunisia

Keyword search frequency data has not been used to suggest any degree of extremist inclination. A wide variety of people may be searching for a particular keyword that returns extremist content, from academics to journalists. Rather, the data has been used as an indicator of how many users are searching for a particular keyword or concept. The searches could have been conducted by both those simply looking for information online or, as is reflected in some of the keywords used, those actively seeking extreme content. Search engines are not exclusively used by extremists, and as such the search frequencies will inevitably include searches by journalists, researchers, students, and others seeking information.

The search frequencies for all the regional and national breakdowns have not been formulated to reflect the percentage of users from a given country. This approach is intended to reflect the true numbers of searches of a given keyword and to highlight the level of enquiry into a given idea.

ARABIC KEYWORD ANALYSIS

The data on Arabic keyword frequencies does not correspond exclusively to the geographical Arab world. Rather, the global keyword frequencies in Arabic include searches by Arabic-speaking internet users worldwide. But with English being the dominant language of the internet, there is an acceptance that English keywords will have greater search frequencies than their corresponding Arabic keywords.

The study also acknowledges that when understanding Arabic search terms, whether globally or regionally, it is in no way an attempt to merge the Arab and Muslim identity, which are of course two separate entities. The reasoning behind choosing Arabic as the language to explore alternative search trends is driven by its inherent relationship with Islam, and also the percentage of the respective populations in the Arabic-speaking regions of the Middle East and North African countries that are Muslim. This figure, according to a 2009 Pew Research Center study, was at around 90 per cent, compared to 24 per cent in the Asia-Pacific region, 30 per cent in Sub-Saharan Africa, five per cent in Europe, and less than one per cent in the Americas.[70]

The comparative analysis of keyword trends in Arabic speaking countries was intended to provide a snapshot of the search trends in a particular country, and indicate the prevalence of a certain train of thought, just as the same data for English keywords in the UK and US were intended to be used.

WEBSITES

Mutually supporting the keyword search frequency work, the websites provided were run through Digitalis' technology to identify all links into each website. CRG provided an initial list of websites to be analysed for linking data. The very nature of the process, which helps identify domains linking into a given website, provides a new selection of domains to choose from to also analyse for linking data. The cyclical nature of this process meant that from the initial list of five websites that were deemed to be extreme, additional websites that warranted further inquiry were identified during the course of the research, taking the total number of extremist websites analysed to 39.

The websites analysed were predominantly those that had been identified as hosting extreme content, including clearing websites,[71] but additionally six websites that were identified as presenting counter-narratives were provided. This brought the total number of websites analysed for linking data to 45.

It was not within the remit of the study to manually investigate every link directed towards the 45 sites as the number of links into the websites ranged from one to over 700,000. However, the linking data did demonstrate certain trends, flag up further websites of interest, and give an indication of the relative strength of the sites.

CONTENT CATEGORISATION

A content categorisation index was created to allow a granular breakdown of the different content types found in the SERPs for the keywords analysed. This also supported the SERP analysis, which looked to analyse the content discovered in the first two pages of each SERP, at a granular level.

The sub-categories were developed to allow for a more detailed picture of the type of content that was found in the SERP. Furthermore, these designations were descriptive of the content found on a particular page and did not reflect a judgement on an entire website. This meant that clearing websites hosting extreme content for analysis purposes were still designated as hosting extreme content, despite not being extreme *per se*.

The extreme content was split into three categories; violent, non-violent, and political Islamist. Websites were categorised as violent if they contained either images of graphic violence or exhortations to violence.

Websites deemed to be extreme but non-violent were those expressing anti-Semitic, homophobic, racist, or sectarian views but without depiction of, or incitement to, violence. The political Islamist category was included to capture political Islamist content which expressed a specific affinity to a particular Islamist group. This allowed for an understanding of the role of these groups in regards to extreme content available online. The distinction in rhetoric between non-violent and political Islamist content may be slight, but for the purpose of this study non-violent extremist content includes sectarian, anti-Semitic, and divisive content put forward by individuals or groups, but more so under the pretext of religious guidance rather than in an effort to gain power. The political Islamist category explicitly refers to known political groups that are actively seeking to gain power, and would include the likes of the Muslim Brotherhood and Hizb ut-Tahrir. Ultimately the distinction between the non-violent extremist and political Islamist categories is the concerted effort to seek political power, despite there being an overlap in the actual ideas put forward.

Websites that neither contained extreme views nor offered counter-narratives were considered to be neutral. This neutral grouping was further broken down to reflect the sources of the content; this included mainstream media websites, clearing and analysis websites, and religious websites.

[70] "Mapping the Global Muslim Population," Pew Research Center, October 2009.

[71] Clearing websites are sites where analysts and researchers can access extremist content for research purposes.

Category	Extreme (X)	Neutral (Y)	Counter-Narrative (Z)	Anti-Islamic (R)
1	Violent			
2	Non-Violent			
3	Political Islamist			
4		News, Analysis, and Religious		
5			Civil Society	
6			Government	
7			Religious Groups	
8				Anti-Islamic

Just as with the categories of extreme websites, the same level of detail was necessary for websites offering a counter-narrative. The counter-narrative types were broken down into three categories to reflect their sources: civil society groups, government, or religious groups. For religious groups, this included known organisations, as well as other efforts that were evidently led by Muslim groups but without being under the banner of a known religious organisation. While it may be difficult to ascertain the exact source of a specific counter-narrative site, (i.e. hard to identify government or civil society backing), the designations were based on what was apparent from a web page's content.

During the course of the SERP analysis, it emerged that for certain keywords there was a consistent presence of far-right extremist content expressing evidently anti-Muslim sentiments. This prompted the creation of an additional category to capture the presence of such content in the SERPs. The same was true of educational sites, which were felt to be outside both the counter-narrative and neutral section.

SERP ANALYSIS

Digitalis and CRG then used the keyword search frequency data and our own expertise to select two samples of keywords for SERP analysis. The first sample consisted of keywords with 500+ average monthly searches in the UK and the second list comprised keywords selected by CRG on the basis of their extreme nature. This sample contained 47 keywords.

The keywords within the sample were then subject to manual SERP analysis. Using the content categorisation index, content identified on the first two pages of Google UK was categorised first by message (extreme, counter-narrative etc.) and then by sub-category, in order to allow for depth of analysis.

Research suggests that 92 per cent of Google traffic is on page one, with page two only receiving five per cent of the traffic and page three an even smaller one per cent.[72] Therefore pages one and two were deemed suitable starting positions.

The end product of this analysis was to categorise all discovered content and gain an understanding of what message the SERP for each sampled keyword was weighted towards, if any, and the relationship of the SERPs relative to a keyword's category. The main objective at this stage was to determine whether a keyword designated as being a moderate or general term could in fact lead users to extreme content, and conversely, to understand if words categorised as extreme were actually generating extreme results or if they were being outperformed by counter-narratives.

For example, it was interesting to note which moderate general keywords allowed access to extreme content. For the purpose of this study, all neutral and anti-Islamic content has been discounted as irrelevant to the ratio.

The end product of this analysis was to categorise all discovered content and gain an understanding of what message the SERP was weighted towards, if any, and the relationship of the SERPs relative to a keyword. For the purpose of this study, all neutral and anti-Islamic content has been discounted as irrelevant to the ratio.

The study accepts there is subjectivity surrounding the effect of anti-Islamic content, as it could be argued such content within a SERP could in fact reinforce certain extreme ideas, and serve to radicalise individuals.

Google Ads, news, and images were discounted from analysis. Google often injects results in to their main results pag-

[72] "The Value of Google Positioning," *Chitika Insights*, 7 June, 2014, http://chitika.com/google-positioning-value.

es as part of their 'Universal Search' algorithm. While to a normal user they are all blended together in the SERP, in reality the information comes from different types of results within Google's indices. For example, Google may inject a News Box into a prominent position in the results, when a significant amount of news is being generated around a related term. However, none of these stories would rank there naturally if it were not for a separate Google algorithm.

IDENTIFYING THE POSSIBILITIES

Digitalis also conducted SERP impact analysis. This was designed to further understand the online landscape in regards to keywords, the content in their SERP, and the ease in which alternative content (in this case counter-narrative) could be introduced. Using data collated across 156 factors known to influence search engine algorithms, Digitalis designated a 'difficulty score' to each SERP, which is the measure of the time and resources required to place content on the first page of results for a given keyword. The difficulty score denotes the following:

- Scores of 20 or less suggest that content referencing the keyword on a relevant site could rank with little promotion.

- Scores of 21-40 suggest that optimised content on a relevant site could rank with promotion.

- Scores of 41-60 indicate a competitive SERP in which it would take promotion of optimised content to achieve a page one ranking.

- Scores of 61+ indicate that there are highly relevant and strong domains ranking for the term and territory in question, meaning assets would require extremely authoritative domains in order to rank.

CONSTRUCTING KEYWORD TABLES

In order to draw all the information gathered together for analysis and report writing, the study constructed 'keyword tables.' These represented, at a glance, a keyword with the following analysis:

- Keyword category
- Geographic search frequencies
- SERP X:Z ratio and therefore the dominant message
- SERP impact analysis

Glossary

IDEOLOGICAL

Apostasy: The abandonment of one's religious belief.

Caliphate: A form of Islamic governance that emerged after the death of the Prophet Muhammad.

Counter-narrative: An alternative message to challenge a widely held idea. May include religious or non-religious messaging.

Dabiq: The title of ISIS' English-language online magazine, named after a town in Syria associated in some Islamic traditions with apocalypse.

Extremism: The desire to impose a belief, ideology, or values system on others to the exclusion of all other views by indoctrination, force, or by seeking to control government.

Fatwa: A non-legally binding edict on Islamic matters issued by a recognised and qualified individual or institution in response to a question.

Hadith: The collection of the reported actions, sayings, and habits of the Prophet Mohammad.

Hizb ut-Tahrir: A global Islamist pan-Islamic movement founded in 1953 that seeks to replace existing systems of governance with a universal caliphate that would rule by its interpretation of sharia law.

Inspire: The title of the English-language magazine published online by al-Qaeda affiliate, al-Qaeda in the Arabian Peninsula (AQAP).

Islamism: A modern religious-political ideology requiring a dominant role for an interpretation of Islam as state law.

Islamist Groups: Modern religious-political groups that seek to establish an interpretation of Islam as state law.

ISIS: Abreviation for the Islamic State of Iraq and al-Sham, a Salafi-jihadi militant group based in Iraq and Syria. The group is referred to by other names, including Islamic State, IS, ISIL, and Daesh.

Jihad: A religious responsibility on Muslims to serve and uphold the religion. The word means 'to struggle' and 'to persevere,' and for the majority of Muslims refers primarily to a spiritual struggle. But for some extremist and Islamist groups jihad is viewed primarily as a violent concept that must be employed to gain political and territorial control.

Kufr: Literally disbelief. More specifically it relates to the denial of God and Mohammad as His messenger.

Nasheed: Literally 'anthem'; vocal music in the form of rhythmic chanting often sung a cappella. They are often used by Salafi-jihadi groups for motivational purposes, but also during celebratory gatherings.

Quran: The central religious text of Islam that is believed by Muslims to be the literal word of God as dictated to the Prophet Muhammad.

Salafism: A Sunni Muslim school of thought that advocates a return to the early Islam practices by the first generations of Muslims, relying on literalist precepts of the Quran, the Sunnah, and Hadith, as interpreted by its adherents.

Shiism: Shia Islam is the second largest denomination of Islam in terms of population, after Sunni Islam. Shia Muslims are also sometimes referred to as Shi'ites in English.

Violent Extremism: The use of physical force or the threat of force by a group or individual to impose or attempt to impose their belief, ideology, or values on others.

TECHNICAL

Content: May refer to any text or multimedia published online.

Internet Service Providers (ISP): A company providing services to access the internet or to host internet content.

Keyword / Search Term: A word or other term used to electronically retrieve data, web pages, or other information from databases; especially in relation to (and exclusively so in the context of this document) search engines.

Linking Data: Linking data identifies all the variant websites that link into, and therefore direct users to, a particular website.

Ranking: Refers to the location of a URL on a SERP, as determined by the algorithm of the search engine in question.

Search Frequency: The average number of searches per month for a particular keyword.

SERPs: Search Engine Results Pages are the pages produced following a search query on a search engine.

SEO: Search Engine Optimisation is the science of promoting a site within search engines with a view to maximising the amount of traffic it receives.

URL: Uniform Resource Locator is a specific character string that constitutes a reference to an internet resource, for example.

APPENDIX

List of Keywords

SERP ANALYSIS KEYWORDS: MOST POPULAR

Apostasy
Apostate
Apostates
Ayman al-Zawahiri
Caliphate
Crusader
Crusaders
Dabiq
Dabiq Magazine
Ibn Taymiyyah
Islamic State
Jihad
Jihad Meaning
Kafir
Khalifa Meaning
Khilafah
Kuffar
Martyr
Martyrdom in Islam
Martyrs
Mujahideen
Shahada
Suicide Vest

SERP ANALYSIS KEYWORDS: HIGH RISK

Abdullah Azzam
Amaq Agency
Apostate Islam
Apostates in Islam
Beheadings
Crusader Army
Crusaders Against Islam
Dabiq PDF
How to do Jihad
Ibn Taymiyyah Jihad
Inspire Magazine
Jewish Coalition
Jihad for Ummah
Jihad in the Quran
Khalifah
Khilafah Syria
Killing Apostates
Killing Infidels
Killing Kuffar
Mujahid
Preparing for Jihad
Rafidah
Soldiers of the Caliphate
Taghut

ABOUT *the* AUTHORS

Mubaraz Ahmed, Analyst, Centre on Religion & Geopolitics

Mubaraz's research focuses on the Middle East and North Africa, with interests including counter-extremism, radicalisation, and modern trends in Islam. Mubaraz studied Arabic and Islamic Studies at SOAS. He has written for Newsweek, The Independent, and has appeared on CCTV America.

Fred Lloyd George, Chief of Staff, Digitalis

Fred's work at Digitalis concentrates on strategic initiatives and cyber security. Prior to joining the Digitalis team, Fred was an Officer in the Welsh Guards serving in several appointments, including an operational tour of Afghanistan in 2012 as a platoon commander, and later as Assistant Equerry to members of the British Royal Family.

ACKNOWLEDGMENTS

The authors would like to thank the staff at the Centre on Religion & Geopolitics (CRG) and Digitalis Reputation for their support and assistance during the production of this report.

The authors would also like to extend a special thanks to Dave King and Emman El-Badawy for providing the opportunity for this collaborative project, and their continued guidance and ideas throughout the research.

It would not have been possible to collect and analyse the wealth of data presented in the report without the knowledge and expertise of Barry Smith.

ABOUT *the* CENTRE ON RELIGION & GEOPOLITICS

Across the world, the interaction of religion and conflict is making its impact felt. Political ideologies and events are exposed to the pressures of religion. Policy makers can no longer ignore the threat posed by violent religious ideologies, but if they are to be defeated, they must be understood.

Through evidence-based reports, media commentary, high-level events, and policy briefings, CRG provides that nuanced understanding. We present informed analysis on the interaction of religion and conflict globally, offering policy options to meet the scale of the challenge.

ABOUT DIGITALIS

Digitalis is an online reputation and intelligence firm with bespoke, proprietary technology which provides rapid, exhaustive coverage of online content about a subject. Our unique, automated analysis facilitates the monitoring and management of online reputation as well as the mitigation of a variety of reputational, privacy and security threats which tend to originate online.

RELIGIONandGEOPOLITICS.org www.digitalisreputation.co.uk