White Paper - The Role of Prevent in Countering Online Extremism

Dr Erin Marie Saltman and Jonathan Russell
2 December 2014

The following White Paper addresses the role of the UK government and social media companies and Internet service providers (ISP) in monitoring and policing the Internet for extremist and/or terrorism-related content. This paper seeks to analyse the effectiveness of the UK government's Prevent strategy and provide recommendations for its improvement in line with the current nature of the threat. Currently, the two biggest challenges for UK counter-terrorism are the radicalisation and recruitment of individuals by the jihadist organisation Islamic State (IS) and the use of the Internet by IS and other extremist organisations to spread unwanted and potentially dangerous ideologies and narratives internationally.

This subject is of great importance, especially as government debates how best to tackle extremism and adequately implement counter-extremism measures both in real terms and online. Sections 2 and 3 discuss the framework of the government's Prevent strategy, while sections 4 through 9 detail the challenges extremism and terrorism-related content online pose. Section 10 addresses the role of Prevent in countering online extremism in the UK.

1. Recommendations

1.1 The UK Government should define the parameters of illegal extremist material, as opposed to legitimate political speech, if the speech and content laws defined by the 2006 Terrorist Act are to be widely understood and enforced both offline and online.

1.2 Counter-extremism and counter-terrorism should be separated at a strategic and delivery level. The UK government must consider the central co-ordination of Prevent, separate from the Office of Security and Counter-Terrorism, with Select Committee oversight, and an in-house due diligence unit and training body. This would enable a national strategy to be applied and implemented across government departments, delivered by local authorities and appropriate institutions. This would also improve accountability and cost-effectiveness.

1.3 It is important to recognise that initial processes of radicalisation predominantly occur offline. While the Internet is an important secondary socialiser and potential catalyst for radicalisation, offline processes must be better addressed in preventative measures, particularly within schools, universities and prisons. Online counter-extremism work must learn from the successes and failures of offline counter-extremism, and coordinate with offline efforts. Prevent is best placed to coordinate, fund, and support online counter-extremism initiatives, as long as the necessary structural changes proposed in 1.2 are implemented.

1.4 Negative measures, including government-backed censorship and filtering initiatives, are ineffective in tackling online extremism, tackling the symptoms rather than the causes of

radicalisation. Motivated extremists and terrorist affiliates can evade such measures easily through the dark net and virtual private networks (VPNs). Blocked materials consistently reappear online and there is no effective way for ISPs or social media companies to filter extremist content.

1.5 Counterspeech and positive measures are critical in challenging the sources of extremism and terrorism-related material online. Community engagement and civil society action are essential components of such positive measures and, as such, counterspeech initiatives should be civil society-led and, in some cases, supported by government through Prevent.

2. Countering Extremism Through Prevent

2.1 The Prevent strategy is one of the four elements of the UK Government's counter-terrorism strategy, CONTEST. Prevent aims to deter individuals from becoming involved in terrorism or supporting terrorism. Following amendments to Prevent in June 2011, the strategy reaffirmed its aims to include the prevention of individuals from becoming involved in non-violent extremist ideologies, recognised as a gateway to violent extremism.[i] This work is carried out at local government levels within communities and coordinated by central government. It is critical to continue tackling extremism of all kinds, and to deliver Prevent locally while strategically coordinating it centrally.

2.2 Revisions to Prevent in 2013 aimed to increase strategy around a) ideology, b) support networks and c) working with other relevant sectors.[ii] The Prevent revisions were primarily aimed at responding to the ideological challenge of terrorism and extremism. Amendments also aimed to provide practical help in preventing individuals from being drawn into extremism/terrorism as well as an aim to work with a wide range of sectors (including education, criminal justice, faith, charities, the Internet and health) where there are risks of radicalisation or which support counter-extremism work. If passed, the 2014 Counter-Terrorism and Security Bill would continue this strategy by putting the involvement of frontline workers in Prevent on a statutory footing, which is a welcome move.[iii]

2.3 In March 2010, the Home Office and the Association of Chief Police Officers (ACPO) produced guidance on the 'Channel' programme, designed to support individuals who have been identified as vulnerable to recruitment by violent extremists. This guidance targets four factors that contribute to making an individual vulnerable to extremist ideologies: a) exposure to an ideology that legitimises or requires violence, often reinterpreting contemporary politics and recent history, b) exposure to people/groups that directly and persuasively articulate that ideology, relating it to a person's background/life history, c) a crisis of identity and/or uncertainty about belonging, often triggered by personal issues, including experiences of racism, discrimination or deprivation and d) a range of perceived sociopolitical grievances, to which there may seem to be no credible and effective non-violent response. While online content and material can be used to contribute to the process of radicalisation, the initial introduction to extremist ideologies continues to be offline, highlighting the importance of community-based Prevent work.

2.4 There remain significant differences between what can be considered legal versus illegal extremism. Illegal extremism includes hate speech, incitement to violence, violent terrorist acts and/or participation or support of a terrorist organisation. While proscribed terrorist organisations such as IS can be approached using the UK's counter-terrorism legislative framework, entryist[1] or

[1] These Islamists engage with and use the current political system in order to weaken it from within and advance their goal of replacing it with an Islamist state. Examples include the Muslim Brotherhood and Jamaat-e-Islami.

revolutionary Islamist groups[2] may not break the law, and should be challenged with a different approach. Islamist extremist organisations, whether legal or illegal, share an ideology that must be challenged through Prevent. Extremism is also not limited to Islamist extremism: Prevent targets a range of potentially dangerous ideologies which includes far right extremism.

3. Analysis of the Prevent Strategy

3.1 By only tackling violent extremism, Prevent struggled to have a meaningful, more long-term impact in its first phase. As many violent extremist organisations are proscribed terrorist entities, incite racial or religious hatred, or promote violence, it is best for other elements of CONTEST to deal with this. Prevent should focus on the causes of this violence, and therefore address the ideological roots of extremism of all kinds, whether violent or non-violent. It must therefore also look beyond the traditional legal tools to counter-terrorism and focus on a strategy that centres on civil society action, engagement with extremist ideologies and narratives, development and dissemination of counter-narratives, and addressing the grievances perceived by those vulnerable to or experiencing radicalisation.

3.2 Without a short-term security focus, Prevent will be able to make more responsible decisions about partnering organisations that are funded through Prevent to deliver counter-extremism work. It remains of vital importance that legal, non-violent Islamist organisations with extremist views are not bestowed the legitimacy of government sponsorship. A failure to appreciate this and insufficient due diligence has meant that public funds, both through Prevent and other grant-making processes, have gone to organisations in the past that oppose the core values of our democratic society and who negatively impact counter-extremism work by adding to the four contributory factors to radicalisation as mentioned. Separation from counter-terrorism and the introduction of a central due diligence unit would avoid such failures.

3.3 The strategy of empowering local government to grant Prevent funding is well-intentioned, as local governments know the particular needs of their region and communities better than central government. However, local structures require more guidance from central government and clearer strategic input on how best to tackle a broad spectrum of extremism. Currently, local governments lack the requisite resources and expertise to produce sufficient due diligence on partnering organisations that they fund to carry out Prevent work.[iv] In line with recent comments by Leader of the Labour Party, Ed Miliband, local community groups and organisations 'have an incredibly important role to play in countering the growth of extremism and stopping people being radicalised'.[v] Centralised due diligence and training would allow for more effective local delivery of Prevent.

3.4 Those responsible for counter-extremism delivery under Prevent, regardless of sector or agency and whether employed by the government or publicly funded to carry out this work as a partner, should receive comprehensive training from a governmentally accredited body that has the expertise to ensure that clarity, consistency and cohesion of the strategy is maintained in the work at the point of delivery. Additional sector-specific training must also be given to improve the effectiveness of the work delivered. The online dimension of counter-extremism (as discussed in Sections 5 to 9) must be

[2] These groups reject engagement with the current political system while also renouncing mass violence. Typically, they instead attempt to build their support (especially amongst members of the military) in the hope that they will eventually be able to overthrow the existing system (potentially through the use of targeted violence) and thereby implement an Islamist state. Hizb-ut-Tahrir falls into this category.

built in to all other aspects of Prevent to deal with the current nature of the threat. A centralised training unit would improve the consistency of the strategy and the delivery nationally.

3.5 The failure of the Department for Communities and Local Government (DCLG) to develop a comprehensive counter-extremism strategy that focuses on countering non-violent extremist narratives has led to insufficient guidance for local government with an over-reliance on the Office for Security and Counter-Terrorism (OSCT) and the police force to deliver Prevent. For this reason, the Home Office, has increasingly favoured counter-terrorism frameworks for tackling extremism, and has sought to change the threshold of legality in this regard. There are existing legal tools to deal with those who have committed terrorism-related offences but there is a danger that similar legal frameworks will be used to target those who sympathise or empathise with terrorism but have not committed an offence. The best way to avoid this, as was intended, is for the responsibility of the development of a counter-extremism strategy to be given to DCLG rather than the Home Office. This would separate the sharp-end work of OSCT and the police to tackle violent extremism from the soft-end work of DCLG and local authorities to deliver counter-extremism projects. As Hazel Blears said, "Prevent…must no longer be viewed as a soft and fluffy end of community engagement, but as a hard, targeted counter-ideological strategy and a counter-narrative that stops people from creating a climate for extremism."[vi]

3.6 Due to the nature of counter-extremism work, it has been very difficult for Prevent to measure its success or cost-effectiveness on a project-by-project basis, on a local level, or on a national strategic level. In contrast, sharp-end counter-terrorism work can be easier quantified in terms of the security impact, the number of terrorist attacks averted, or the prosecution rates for terrorism-related offences. This imbalance leads to the questionable conclusion that sharp-end counter-terrorism is more effective than soft-end counter-extremism and is therefore worthy of greater investment. More effort must be made through Prevent to measure outputs and outcomes of counter-extremism work.

3.7 Prevent work is necessary in a range of sectors such as schools, universities, prisons and communities where there are risks of radicalisation. If adopted, the proposals in the 2014 Counter-Terrorism and Security Bill will implement this, but they must be accompanied by strategic and structural changes in Prevent to develop and effectively implement a coherent strategy to counter non-violent extremism. Delivery of counter-extremism work in these sectors varies tremendously leading to considerable confusion among Prevent practitioners and communities involved in Prevent. A clearer strategy would avoid such confusion and tension in this vital domain,[vii] improve the effectiveness of, and decrease reliance on, those carrying out sharp-end counter-terrorism work such as the Police or the Intelligence Agencies, and improve effectiveness without the need for the over-securitisation of institutions such as schools. This should include an online dimension to Prevent, to develop online counter-extremism initiatives to mirror offline efforts.

3.8 It is also important that those carrying out sharp-end counter-terrorism work understand the necessity and importance of soft-end counter-extremism efforts. Counter-extremism work to challenge extremist ideologies is necessary in tackling longer-term goals of preventing individuals from radicalising to the point of violent extremism. In particular, efforts must be taken by decision-makers to strike a balance between national security and civil liberties. We have seen that failure to do this adds to the perceived grievances of those vulnerable to extremism and radicalisation, and allows extremists to feed these domestic grievances into their narrative of the West's ideology being at war with Islam.

3.9 There remains little oversight of Prevent from elected representatives. We recommend the establishment of a Select Committee to improve the credibility of Prevent, constantly reevaluate its

effectiveness in light of the current nature of the threat, and to ensure that there is a cross-party approach to tackling extremism. This is necessary to bridge the complex combination of centralised strategy and local delivery, and will provide democratic oversight and increased transparency.

4. Countering Extremism and Terrorism Online – Negative Measures

4.1 Illegal terrorist-related content is taken down in the UK through three channels: a) by civil-society user-led flagging, b) ISP and social media platform-led initiatives and c) a top-down process of government take-down requests.

4.2 Content that breaches platform regulations with regards to terrorist-related material is also actively assessed by social media platforms without prompting from national government agencies or security services. Many leading social media companies have teams that actively research, analyse and take down content that is determined to go against platform guidelines. Often, the content taken down proactively by internal security services is more than the amount of content taken down through government flagged content.[3] While structures vary slightly, leading platforms have working relations with the UK government security services to address terrorist-related content as a priority.

4.3 The CTIRU, formed in early 2010 by the Association of Chief Police Officers (ACPO), was set up to 'remove unlawful terrorist material content from the Internet'.[viii] The CTIRU is the primary UK government body dealing with online extremist and terrorist-related content by a) removing unlawful content, b) serving Section 3 Terrorism Act notices within the UK c) alerting online terrorist offences falling under other government units' jurisdiction such as Counter Terrorism Intelligence Units and the Metropolitan Police Service Counter Terrorism Comment.[ix] Due to the impracticality of serving notices on Internet-users, there are currently no public records showing Section 3 Terrorism Act notices served by the CTIRU.[x]

4.4 Subsequently, the unit's primary action has been facilitating the take-downs of terrorist-related materials online. Currently, the CTIRU estimates weekly take-downs of 1,100 pieces of content breaching terrorist legislation, with over 70 per cent of this material relating to events taking place in Syria and Iraq.[xi] The CTIRU have become increasingly active in working to take down content that goes against Terrorist Legislation. While the CTIRU have worked to take down an estimated 49,000 pieces of content in total since its formation, more than 30,000 pieces of content were removed since December 2013 to October 2014. However, there is lack of clarity over the content and context of the material that has been removed and no further information about how many of these take-downs are duplicates or re-posts has been given.

4.5 In order for the CTIRU to have a piece of content taken down from social media platforms, there are user-based flagging systems. Leading social media platforms have structures for users to flag content they believe is contentious or illegal and give a small explanation as to why. The main social media platforms also work with government officials and security units through priority flagging systems or through specific reporting streams so that government targeted content is given priority for review by social media companies.

[3] The reason that internal Social Media-led take downs is often more than CTIRU-flagged content is because Social Media platforms are working with their broad international teams all addressing groups and organisations that have been deemed violent or terrorist in their nature. In this way, once a Social Media platform has flagged a group as illegal on their platform, regardless of whether or not the UK has officially proscribed the group in question, the platform will remove all content linked to the violent extremist or terrorist group and affiliated content. Information from discussions and interview with representatives from Twitter, Facebook and Google.

4.6 All flagged/targeted content is peer reviewed by social media personnel to assess whether or not the material does in fact violate the regulations set forth by the social media platform in question. Content found in violation is suspended/blocked/removed while content that is not seen to violate regulations is left.[xii] Currently, there is a working relation between CTIRU and social media platforms as well as ISPs. The UK's security relations with social media companies are highly functional even compared with other European countries.[xiii]

4.7 Extremist and terrorist-related online content can be addressed in three ways: negative measures, positive measures and monitoring. Negative measures are methods, which block, censor, filter or remove content by various means so that the unwanted and/or illegal content is no longer accessible. Positive measures are any actions which work to, rather than remove content, counter the messaging and/or propaganda being espoused in the contentious material. This can be done through a variety of means discussed below. Lastly, monitoring entails leaving content up but using the material as a means of analysis that can assist in counter-terrorism or counter-extremism efforts, although not all companies do this.

5. The Effectiveness of Negative Measures

5.1 Despite the UK government currently relying heavily on negative measures to counter terrorism online, there is a large body of evidence that shows the overall ineffectiveness of blocking, filtering and taking down content.[xiv] Negative measures alone do not adequately tackle broader extremist trends, nor do they contribute to an overall depletion of terrorist-related materials available online. There are many examples of this, in particular relating to the terrorist group IS, where material is being rapidly taken down by social media platforms only to reappear just as quickly. Furthermore, many Internet services are based overseas and have no presence in the UK and therefore have no compulsory agreement with UK law enforcement.

5.2 A prime example of this was the re-emergence of the gruesome James Foley beheading video that was re-posted and redistributed through various video platforms and shared on a myriad social accounts. Research has shown that accounts of individuals claiming to be members of IS and/or supporting IS that have been blocked/suspended rapidly reform under slightly modified names and are able to re-amass large quantities of followers within a short amount of time.[xv] Research has also shown that as certain social media platforms are seen as less accessible for extremist and terrorist networks, these targeted actors are seen moving to less restrictive and more anonymous platforms, such as Vkontakte, Kik and Snapchat.[4]

5.3 For this reason, increasing negative measures to include 'extremist content', which has yet to be fully defined in legal terms, would push a larger network of online users to seek platforms which might be less willing to work with the UK government. These may be platforms based in non-UK jurisdictions or on smaller anonymous networks. Expanding negative measures to include unwanted extremist content that does not breach defined legal terms, would also push users that feel targeted into the dark web where monitoring is no longer possible. This increases security risks if counter-terrorism and counter-extremism practitioners are impeded from monitoring and surveillance. Finally, expansion of the government's role in negative measures may lead to public perception of the government policing

[4] Examples of this can be seen in the extremist organisation, Al-Muhajiroun (and all its subsequent reincarnations) declaring openly that Facebook should not be used because it exposes networks too easily. There has also been a recent online migration to smaller social media platforms.

thought. This perception of western tyranny and hypocrisy, already used within extremist/terrorist propaganda, is exploited for radicalisation and recruitment purposes.

5.4 Recent suggestions discussed at a government level have also implied that extremist and terrorist-related content can be filtered in a similar manner to Child Sexual Abuse Imagery (CSAI). However, the nature of extremist and terrorist-related content makes broad filtering structures and data-bank algorithms impossible. CSAI is deemed illegal in the making, distribution and viewing of CSAI content. The same cannot be said for extremist and terrorist-related content. Firstly, the vast majority of contentious extremist and/or terrorist-related content is written, requiring the interpretation of the reader to deem whether or not messaging breaches legality. Secondly, even images which relate to and/or document terrorist activities (violent or otherwise) cannot be broadly defined as illegal. Media, as well as counter-extremism practitioners, both use images and content that might be labelled as 'extremist' or 'terrorist-related' under a different setting. Even the US State's Department's online counterspeech campaign, #ThinkAgainTurnAway, uses IS content but changes the messaging so that it works against IS propaganda. For this reason, broad filtering measures are both technically and legally contentious, and practically impossible to implement.

6. Countering Extremism and Terrorism Online – Monitoring

6.1 Monitoring and surveillance of extremist and terrorist-related materials online is conducted at both the government and NGO/think-tank level. While explicit terrorist-related and illegal materials should be dealt with through pre-existing legal structures, open source 'extremist material' or content which is not deemed illegal by government should instead be monitored, offering a great deal of intelligence and data for security services, counter-terrorist practitioners and counter-extremism practitioners.

6.2 On a governmental level, monitoring and requesting data that goes beyond what is easily accessible online requires a process of information retrieval outlined in the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA gives guidance procedures that must be followed before interception of communications can take place in the UK. Only specific UK government security directors, chiefs or commissioners holding office can issue a RIPA interception warrant.[xvi] Interception warrants must be deemed necessary on the criteria that requested information is a) in the interest of national security, b) for the purpose of preventing or detecting a serious crime or c) for the purpose of safeguarding the economic well-being of the UK and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.[xvii] Social media companies work with governments through RIPA to assess information that can be given to the UK government for security monitoring or eventual take-down purposes.

6.3 Due to the transnational nature of the Internet and extremism, there is greater need for coordinated international action in this area, rather than unilateral activity in one country alone. There are numerous models that can be seen as a basis for effective coordinated action such as the Inhope model for Child Sexual Abuse Imagery as well as the ongoing work of EU Commissioner Cecilia Malmström and Gilles de Kerchove on counter-extremism and counter-terrorism.

6.4 It remains the case that radicalisation processes start with the introduction to extremist ideologies that then lead to violent extremism and potential terrorist acts. Acts of terror are either planned within the UK or, more recently, have been leading individuals abroad to join terrorist organisations. Introductions to extremist ideologies and the 'first sparks' of radicalisation remain prevalent offline

where recruiters and extremist sympathisers target vulnerable individuals.[xviii] As such, the Internet serves as a catalyst and a tool for radicalisation processes and recruitment.

7. The Effectiveness of Monitoring

7.1 Monitoring extremist and terrorist trends online, particularly using social media as a tool for visualising networks, has been crucial in recent surveillance as well as counter-terrorism and counter-extremism initiatives.[xix] Not taking down extremist content that does not breach counter-terrorism legislation is a valuable way for governmental and non-governmental practitioners to build a more accurate picture of the radicalisation process to improve strategies to tackle it.

7.2 Monitoring of extremist and terrorist-related materials is also highly effective through NGO and think tank channels. Dedicated organisations in the UK monitor this area of online activity in order to better understand current social and political movements and inform governments and the wider public about trends. This is of high importance to better understand the processes and trends in radicalisation that lead to violent extremism and terrorism. Only in understanding these processes and targeting sources can these processes be better prevented, deterred and addressed by both government and civil actors. Mapping online extremism will also allow for more effective targeted prevention work through Prevent.

8. Countering Extremism and Terrorism Online – Positive Measures

8.1 A number of public, private and government initiatives have come about in recent years to actively counter extremist messaging online. There are two types of positive measures currently taking place: a) online initiatives that are dedicated to challenging extremist and or terrorist narratives and b) websites and/or organisations that confront a wider range of religious and/or political issues which include counterspeech messaging.[5] Counterspeech messaging can be divided into three categories: a) content that aims to directly negate and undermine the content being put forth by extremism and terrorism-related messaging, b) counterspeech that positively offers other narratives/alternatives/options and c) counterspeech which aims to purely inform and provide transparency around an issue that is monopolised and/or misinterpreted by extremism and terrorism-affiliated individuals.

8.2 The UK government does not currently develop its own counterspeech content, although some governments have begun to develop programmes from within security units. The most well-known example of this is the US State Department's Centre for Strategic Counter-Terrorism Communications-led initiative discussed in 6.4 using the #ThinkAgainTurnAway campaign. However, government counterspeech is limited in its effectiveness. Research has shown that the three vital factors in successfully reaching target audiences through counterspeech are the message, the messaging and the messenger.[xx] When the government is the messenger, target audiences are often less likely to see, believe or positively respond to the message. For instance, government messaging is unlikely to meaningfully reach younger individuals that are vulnerable to extremist propaganda and processes of radicalisation because that audience tends to view the government as an icon of authority, hence it is already viewed with scepticism by the target audience.

[5] Counterspeech can be defined as any articles, videos, speeches and other material that seeks to challenge hateful and/or extreme views through positive messaging and narratives.

8.3 Extremist propaganda tends to target governments as oppressive state forces. For this reason, government counterspeech is best produced to give transparency around an issue and clarify government stances on specific topics that are targeted by extremist voices, rather than being seen to 'argue' against propaganda. Government counterspeech that argues directly with extremists may be perceived as the government lowering itself to the extremists' level.

8.4 Islamist extremist propaganda uses a range of voices including extremist preachers to justify a religious narrative, and foreign fighters and jihadists to justify their cause. For this reason, credible messaging to a target audience is best created by an equally wide range of credible non-extremist voices coming from civil society level. Civil society is best placed to provide counterspeech that both negates the extremist message directly, as well as provides counterspeech that can provide vulnerable target audiences with alternatives to extremism.

9. The Effectiveness of Positive Measures

9.1 In recent years, and particularly in response to the current crisis in Syria and Iraq, there have been a number of counterspeech campaigns and positive measures taken to counter Islamist extremist trends. Some groups/campaigns/organisations work specifically to address extremism while others have more broad goals that include countering extremism.

9.2 Examples of organisations that target extremism directly in the UK include *Counter Extremism Project* – a non-profit international organisation made up of international leaders; *Inspire* – dedicated to counter-extremism and gender inequality and responsible for the #MakingAStand campaign; *Stand for Peace* – an interfaith organisation aimed at tackling extremism and; the *Against Violent Extremism* (AVE) network – using ex-extremists to tackle radicalisation processes and challenge extremist messaging. There are also many examples of individuals and decentralised actors that are not part of any formal organisation that have come together and united to counter Islamic State more recently both on and offline. An excellent example of a decentralised counterspeech campaign that went viral was the #No2ISIS social media campaign.

9.3 It is important that the government reconstructs how it defines deliverables and moves away from implementing extra negative measures that have proven to be ineffective in the overall goal of countering radicalisation processes and/or making terrorist-related content or communication online less accessible. Positive measures that challenge extremism are more effective compared to negative measures because they are able to: a) target specific audiences thought to be vulnerable to extremism, b) measure and track viewership trends and c) co-ordinate with Prevent's offline counter-extremism initiatives.

9.4 Negative measures that counter online extremist and terrorist-related content often result in the same content reappearing on a variety of platforms repeatedly. This is one of the leading reasons why counterspeech initiatives, challenging extremist ideologies directly, are more effective. Following social media trends in terms of viewership numbers, responses to counterspeech campaigns and networking between counterspeech producers can all be measured and monitored.

9.5 Civil society is much more effective in challenging extremist and/or terrorist propaganda streams as, in essence, extremist movements are themselves peripheral civil society movements. However, that is not to say that the government and private sector do not have a large role to play in facilitating and monitoring counterspeech initiatives. Governments play a key role in providing infrastructure that encourages and supports counterspeech initiatives. Government support can be implemented

through financial assistance and incentives given to organisations/movements/communities that are putting forward targeted counterspeech. The government should also facilitate counterspeech initiatives structurally through Prevent and co-ordinate online and offline efforts to counter extremism.

9.6 Private sector companies, particularly social media companies and ISPs, can also work to facilitate counterspeech in a way that provides tangible deliverables to counter-extremism. These private companies benefit from supporting counterspeech content as a means of countering online extremism since it creates a healthier realm of ideas within their platforms and naturally develops a more hostile environment for individuals wanting to use online platforms for extremist and/or terrorist-related purposes.

10 Prevent and Online Extremism

10.1 It is clear that the radicalisation phenomenon is very similar, whether online or offline, and that the Internet is simply a vehicle for giving exposure to extremist ideologies. The Internet must therefore be seen as a valuable tool to be used in challenging extremism (both violent and non-violent) and terrorist organisations.

10.2 Prevent must actively respond to the need to countering online extremism. As identified in Quilliam's 2014 report *Jihad Trending*, Islamist extremist organisations are increasingly adept at using the Internet. IS is a prime example of unprecedented online propaganda distribution and active social media usage to disseminate its messaging, further radicalise those vulnerable to extremism, and recruit supporters to the organisation. This has posed a new threat to European countries, including the UK, with over 500 British citizens having traveled to Iraq and Syria as foreign fighters. There is also a highly significant amount of non-violent extremist content available online and shared on social media platforms which needs to be better challenged while remaining in a legal space of discourse.

10.3 The Internet presents numerous difficulties for lawmakers, given the lack of national borders online. Even though it is illegal in the UK to promote or glorify terrorism online, it is often the case that the offender or website used is based in a foreign jurisdiction. Encryption may also prevent the offender's identity being known to prosecutors. Furthermore, it is increasingly the case that illegal material is shared, not on static websites owned by the offender but on social media platforms, meaning that private companies, often also in foreign jurisdictions, are then asked to remove the content rather than authorities being able to remove entire websites. As such, traditional legal tools are outdated when it comes to counter-terrorism policing online. Given that legislative tools should not be used for legal content, and are ineffective at dealing with illegal content, we must find a solution away from the legal framework of counter-terrorism but within the strategic policy framework of Prevent.

10.4 Given the breadth and range of extremist content online, it is not possible to develop algorithms that can accurately identify all illegal material, let alone all extremist content. Even if it were morally or legally justifiable, it would be unfeasible for a computer to build a bank of extremist content for deletion, and it would be ineffective as the extremist content is likely to reappear in another format. Extremism must be dealt with by human engagement, as its definition, like that of terrorism, is heavily dependent on context. Moreover, the causes of extremism and the factors of radicalisation as identified above should be tackled if we are to see a reduction of the amount of extremist content.

10.5 Research has also shown that as increased activities by marginalised and periphery groups, including extremist and terrorist-related networks, are deterred or censored on mainstream social media platforms, there is a movement towards using the dark net by using Tor and Internet access through VPNs. This makes the monitoring and surveillance of more extremists less possible. Prevent must play a larger role in challenging extremist ideologies and narratives online that could deter individuals from engaging further with extremism, and on unmonitored parts of the Internet.

10.6 The development of an online dimension to Prevent would not only bypass the need to police the Internet, it would also challenge online extremism more effectively. At a primary prevention level, Prevent must improve digital literacy and critical consumption education to build resilience of those vulnerable to extremism. In terms of targeted prevention, Prevent must develop and disseminate credible counter-messaging to tackle the ideologies, narratives and propaganda of extremist organisations, as well as addressing the grievances perceived by those vulnerable to extremism. Prevent must take its civil society approach online by building a broader-based human reporting structure and training practitioners to flag or report illegal terrorist content.

10.7 The 2014 Counter-Terrorism and Security Bill recommends that the Channel Programme gains a statutory footing.[xxi] Referrals for ideological engagement, mentoring, deradicalisation, rehabilitation and reintegration would be as welcome online as it is offline. If Prevent were to add an online dimension to its work, Channel would be perform a necessary function for those who disseminate extremist material online.

11. Conclusions

11.1 The central co-ordination of Prevent would improve the clarity, consistency and cohesiveness of the strategy for practitioners and recipients. This would mean counter-extremism remains distinct from counter-terrorism, prompt the development of a strategy to counter non-violent extremism, reduce the workload of the police by coordinating the delivery of Prevent, improve consistency of delivery across local authorities and across government departments and agencies, employ a due diligence team to improve the effectiveness of spending under Prevent and manage a training team to ensure the appropriate resources are given to all Prevent practitioners. It would also allow the efficient development of an online counter-extremism strategy to complement offline efforts.

11.2 The continuation of communication and working channels between government, social media companies and ISPs is key to continuing the current efforts being made to remove content which is deemed illegal under UK terrorist legislation and more broad regulations against Hate Speech and Incitement to Violence. However, as discussed, negative measures do not tackle the roots of problems concerning processes of radicalisation and the existence of terrorist networks online. Therefore, while negative measures should target explicitly illegal content, there needs to be a more robust infrastructure of monitoring and positive initiatives that challenge extremist and terrorist-related propaganda and narratives.

11.3 Surveillance and monitoring of extremist and terrorist-related content should continue through government and intelligence sectors. Monitoring and analysing extremist and terrorist-related trends should also be encouraged by think tanks and NGOs which can provide important data and insight into processes so that targeted messaging is more effective. Surveillance can also benefit higher accuracies in risk assessments concerning real versus perceived threat levels.

11.4 Prevent should develop an online sphere to its strategy, using positive measures to counter extremism online. Counterspeech can be measured for effectiveness and cost-effectiveness through viewership trends, targeted campaigns and through the range of key organisations becoming involved in the production of counterspeech content, delivering messaging from a range of credible voices. Counterspeech initiatives are ideally delivered by civil society and supported through Prevent.

Endnotes

[i] See: *Prevent Strategy*, Presented to Parliament by the Secretary of State for the Home Department, (HM Government: June 2011), < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf>, accessed 12 October 2014.

[ii] See: 'Prevent: 2.44', *CONTEST: The United Kingdom's Strategy for Countering Terrorism – Annual* Report, Presented to Parliament by the Secretary of State for the Home Department (March 2013), p. 21, < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf>, accessed 5 November 2014.

[iii] Counter-Terrorism and Security Bill, http://www.publications.parliament.uk/pa/bills/cbill/2014-2015/0127/cbill_2014-20150127_en_1.htm (November 2014)

[iv] This has also been the case since Prevent funding had been drastically decreased from £17 million in 2010 to £1.7 million in 2013 in parallel to decreased funding for police work tied to Prevent falling from £24 million to £18.7 million. Many programmes were also cut during this time, including in Greenwich where the Woolwich perpetrators resided. See also: 'Funding for anti-terror programme cut by 90%', *ITV* News, 8 June 2014. http://www.itv.com/news/update/2014-06-08/funding-for-anti-terror-program-cut-by-90/

[v] Ed Miliband Comments at PMs Oral Question Session 25 Nov 2014. http://www.theyworkforyou.com/debates/?id=2014-11-25a.747.0&s=speaker%3A10048#g757.3

[vi] Hazel Blears Comments at PMs Oral Question Session 25 Nov 2014. http://www.theyworkforyou.com/debates/?id=2014-11-25a.747.0&s=speaker%3A10048#g757.3

[vii] *CONTEST: The United Kingdom's Strategy for Countering Terrorism – Annual* Report, Presented to Parliament by the Secretary of State for the Home Department (March 2013).

[viii] Main page of the *Counter Terrorism Internet Referral Unit*. Link found at <https://www.herts.police.uk/advice/counter_terrorism.aspx>, accessed 10 November 2014.

[ix] As discussed on the CTIRU main page. Ibid.

[x] As of October 2013, public documents stated that the CTITU Unit had, since its creation, never issued a Section 3 Terrorism Act notice. See: *Freedom of Information Act*, (Metropolitan Police: Total Policing, October 2013), <http://www.met.police.uk/foi/pdfs/disclosure_2013/october_2013/2013010000385.pdf>, accessed 9 November 2014. Note: Document produced without reference number. See reasons: Stated September 2011 "8.1.13 There have been no formal notices issued under section 3 in order to remove any material. All removals have been conducted voluntarily by the hosting company/website administrator. The existence of this formal process does however allow the CTIRU to have recourse where negotiations with industry falter" 'Memoranda to the Home Affairs Committee: Post-Legislative Scrutiny of the Terrorism Act 2006', *Secretary of State of the Home Department*, (September 2011), p. 9.

[xi] See: Mark Townsend and Toby Helm, (2014) 'Jihad in a social media age: How can the west win an online war?', *The Guardian*, (23 August) < http://www.theguardian.com/world/2014/aug/23/jihad-social-media-age-west-win-online-war> accessed 10 November 2014.

[xii] Refer to regulations of main social media platforms such as Facebook < https://www.facebook.com/communitystandards>, Twitter < https://support.twitter.com/groups/56-policies-violations> and YouTube < https://www.youtube.com/t/community_guidelines>.

[xiii] Discussing the rates of government requests for taking down content leading to Social Media companies taking down the actual content, the UK rate of compliance is much higher than other European nations. Through open access documentation we can see that in the UK Facebook compliance with Government information and take-down requests is over 70% (See: 'United Kingdom Requests for Data', *Facebook Government Requests*, (January – June 2014) <https://govtrequests.facebook.com/country/United%20Kingdom/2014-H1/?> accessed 10 November 2014). This can be compared to countries like France which has just over 30% validity in its request-making. The rate of compliance is thought to be even higher within Google compliance responses.

[xiv] See: Ghaffar Hussain and Erin Marie Saltman (2014) *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It*, (Quilliam: London). See also: Peter Neumann (2012) 'Countering Online Radicalisation in America', *Bipartisan Policy Center*, (Washington DC).

[xv] See: Erin Marie Saltman and Charlie Winter (2014) *Islamic State: The Changing Face of Modern Jihadism*, (Quilliam, London), pp. 41-42.

[xvi] For a list of UK security officials that are able to issue a warrant under RIPA guidelines see: 'Interceptions of Communications: Code of Practice', *Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000*, (Home Office: 2007), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf>, accessed 11 November 2014.

[xvii] Ibid, Section 2.3, p.7.

[xviii] Certain environments are more vulnerable to attract extremists wishing to recruit than others. Universities, prisons and local religious communities are often targeted by recruiters. See: Ghaffar Hussain and Erin Marie Saltman (2014) *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It*, (Quilliam: London), <http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/jihad-trending-quilliam-report.pdf>, accessed 27 May 2014.

[xix] Various think tanks and counter-extremism centres have been using new technologies and mapping software, like Gephi, to show international terrorist sympathiser networks and help calculate the nationalities and numbers of foreign fighters we are currently seeing in Syria and Iraq. See: Joseph Carter, Shiraz Maher and Peter Neumann (2014), *#Greenbirds: Measuring Importance and Influence in Foreign Fighter Networks*, (ICSR), <http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf>, accessed 5 July 2014.

[xx] See: (2014) 'Online Extremism: Challenges and Counter-Measures Analysis', *Eurasia Review*, (11 November) < http://www.eurasiareview.com/11112014-online-extremism-challenges-counter-measures-analysis/> accessed 11 November 2014

[xxi] Counter-Terrorism and Security Bill, http://www.publications.parliament.uk/pa/bills/cbill/2014-2015/0127/cbill_2014-20150127_en_1.htm (November 2014)