JOURNAL FOR DERADICALIZATION

Summer 2019
Nr. 19
ISSN: 2363-9849

Exploring the capabilities of Prevent in addressing radicalisation in cyberspace within Higher Education

Liam Sandford[a1]
[a]Policing Strategy Unit, Thames Valley Police; School of Natural and Social Sciences, University of Gloucestershire

Abstract
The Counter Terrorism and Security Act (2015) introduced a binding duty on public sector bodies in the United Kingdom (UK), including education, to have 'due regard to the need to prevent people from being drawn into terrorism'. The Prevent duty has become widely controversial in the Higher Education (HE) sector with questions as to whether it contravenes academic freedom and freedom of speech.
This research seeks to identify how Prevent may be applied to cyberspace to reduce risk of students being radicalised online at universities. Through semi-structured interviews (N= 16) with individuals working in Prevent and HE, attention is given to the capability of monitoring and filtering website content, which must be considered by universities as part of Prevent compliance. In addition, non-technical methods of reducing radicalisation in cyberspace are explored. Consideration is given to building students' resilience to challenging information they see online through developing counter-narrative content for social media platforms. With students developing counter-narrative content themselves, specifically addressing vulnerability drivers to radicalisation, universities can enhance compliance with Prevent and create counter extremist content which can be used in cyberspace both in and outside of HE.

Article History
Received May 16, 2019
Accepted June 16, 2019
Published June 28, 2019

Keywords: Prevent Duty, Counter Terrorism, Radicalisation, Higher Education, Counter-narratives

Introduction

Development of cyberspace and global communications has vastly changed the way the world operates, enhancing both business relationships and criminal networks. Considine et al (2016) discuss the revolution of technology as coming with 'uses and abuses' which have benefited terrorist organisations in seeking to recruit individuals to support their cause. Solutions to

[1] Corresponding Author Contact: Liam Sandford, Email: liam.sandford93@gmail.com; Twitter: @liamsandford

tackling radicalisation online have been scrutinised in the media, with suggestions that powerful cyber companies, such as Google and Facebook, should have better strategies to deal with an online terrorist presence (Guiora, 2018). One initiative that could be applied is Prevent, the strand of the UK Government Counter Terrorism Strategy (CONTEST) that deals with individuals in the pre-criminal space (Heath-Kelly and Strausz, 2018).

Prevent has been in place since 2006 but was made compulsory for public sector bodies in 2015, including universities (Counter Terrorism and Security Act, 2015). The jurisdiction of Prevent is predominantly in England and Wales for the Higher Education (HE) sector. Although Scottish universities are bound by the duty their guidance is separate from that of England and Wales, and their duty is overseen by the CONTEST Scotland Board as opposed to the Office for Students (Prevent Duty Guidance for HE in Scotland, 2015). The Prevent duty does not apply to Northern Ireland. Some of the controversy associated with Prevent in HE stems from the view that university staff are being asked to 'monitor Muslim moves' (Pal, 2015) and act as 'state instruments of surveillance' (Elton-Chalcraft et al, 2017). It is important, however, to acknowledge that the duty is bound to the university as opposed to those working at the institution, and therefore not requiring staff to surveil students. The duty states that a university must have 'due regard to the need to prevent people from being drawn into terrorism' (Counter Terrorism and Security Act, 2015).

Prevent implementation at universities has been controversial with views that it is a mechanism to target Muslim student communities (Acik et al, 2018). The National Union of Students (NUS), in particular, have been known to promote anti-Prevent campaigns, such as 'students not suspects' and 'preventing Prevent' (NUS, 2015), both of which are based on the premise that it is disproportionately targeted at Muslims (Miah, 2017). Students' Unions (SU) are not bound by the Prevent duty, making it difficult to engage students where the SU adopt the NUS stance. Although most universities implement Prevent as safeguarding, negative media and misinterpretation of the policy shape misled stereotypes of Prevent, causing challenges for implementation in cyberspace.

The relationship between Prevent and cyberspace has not been well established, in particular for universities. Prevent Duty Guidance for HE (2015) outlines that monitoring and filtering of website content on the university servers must be considered. By undertaking 16 semi-structured interviews with specialists in Prevent and HE, consideration is given to potential implementation of Prevent in cyberspace at universities. Some participants offered views on whether monitoring and filtering could stop radicalisation online whilst others discussed the use of counter-narratives as an alternative.

Terrorist use of cyberspace

A power shift from Al Qaida to Daesh has seen a change in modus operandi (MO) for terrorist recruitment, with increased use of cyberspace (Theohary and Rollins, 2011; Goodman et al, 2007). Daesh have carried out numerous attacks in Europe and rely on recruiting lone actors through social media to carry out their objectives (Cozine, 2016). Technology developments have been exploited and in virtual interaction, Daesh are seeking to achieve what Awan (2017) describes as the 'cyber jihad'. There are multiple opportunities that cyberspace offers terrorist organisations to enhance the 'cyber jihad', most of which will induce fear into the public (Santoro, 2018). This is particularly evident when Daesh claim responsibility for attacks in which there is no evidence to suggest their involvement, such as the mass shooting in Las Vegas in October 2017. With high popularity of social networks, individuals can share information worldwide instantaneously post event, making the ability to stop information at source problematic. Recent attacks, in New Zealand and Sri Lanka, have seen social media used to broadcast an attack, and be shut down in order to stop the spread of misinformation about the attacks. Questions have been raised as to whether this was a sensible approach and arguments condemning filtering social media have revolved around freedom of speech. Bertram (2016) argues that governments have the responsibility to use social media more effectively to counter terrorist content online.

There is much debate around the responsibilities of global cyber companies, or governments to manage such use of the internet (Abdulhamid and Ibrahim, 2014; Bertram, 2016; Wolff and Lehr, 2018), making the discussion wider than solutions within HE. In attempts to create counter extremist strategies Google, partnered with the Institute for Strategic Dialogue (ISD), launched an innovation fund to develop online projects that seek to counter extremist narratives. The impact of the innovation initiatives is unknown due to the fund only being in its infancy; however with projects such as 'virtual inclusion: tackling hate and extremism in the UK using virtual reality technology' (ISD, 2019) it is encouraging that new technology is being explored to understand the capabilities it may have in combatting radicalisation.

Despite the direct approach of Daesh use of social media, it is the indirect discussion from the public which inadvertently assists terrorism when information relates to extremism (Weimann, 2014). Xie et al (2016) identify that, social media posting increases following a tragic world event, in both fear and reaction to attacks (McQueeney, 2014). In reaction to the Paris attacks in 2015 Facebook created a 'profile picture cover' of the French flag in support of victims (Ribeiro, 2015). Whilst this was intended to support the victims of those attacks, the opinion that such a strategy raises the profile of terrorism has not been commonly shared (Costa, 2015). The changing of profile pictures, and similar social media activity, is often combined with uninformed opinions (Zelenkauskaite and Balduccini, 2017), which can add to the terrorist narrative, or lead to more people seeing terrorist content online. The widespread of terrorist material on social media makes it difficult to control and is problematic for organisations trying to combat extremism in cyberspace. Thorne (2015) postulates that social media posts as a source of information should be treated with an element of caution because opinions can provide people with false knowledge (O'Connor et al, 2016). Where false knowledge and inability to challenge information meet, misinformation is likely to form the basis of opinions. Zucker (2019) suggests that critical thinking could be used to address the ability to challenge information. Through the use of education the application of critical

thinking could help individuals build resilience to negative influences, including both misinformation and radicalisation.

Considering monitoring and filtering – Prevent's solution for cyberspace at universities

Universities are required to have an information technology (IT) policy which relates to their approach to Prevent in cyberspace. Monitoring and filtering of website content on university servers must be considered as part of the policy (Prevent Duty Guidance for HE, 2015). Monitoring is the process of observing the content individual's access online, with a purpose of identifying who is viewing undesirable material (Hare, 2017). Filtering blocks websites that should not be accessed by individuals using that particular server (Wright and Breindl, 2013). Streitwieser et al (2019) highlight that it is unusual for policy to provide specific recommendations for universities to implement in relation to countering radicalisation; however, although consideration has to be given to these methods, they do not have to be implemented.

Isaacson (2016) discusses how cyberspace is a 'freeway' that cannot be controlled because once information is shared on the internet it can always be traced. The lack of boundaries in cyberspace leaves the control of available content a difficult task for a university. Monitoring and filtering are methods used in schools and colleges (McNicol, 2016); and, it may be thought that, due to its use in under-18 education, it may also work effectively in HE. Blocking content and watching what staff and students access on the university server is limited (Lee et al, 2005), and, with the ability to use 3G or 4G network access, monitoring and filtering can be easily averted (Aloi et al, 2014). Having technical barriers to Prevent does not mean that universities cannot make a difference to countering radicalisation in cyberspace, and consideration should be given to whether paying 'due regard' (Counter Terrorism and Security Act, 2015) is about meeting compliance, or making a wider difference to countering extremism.

For universities the factor of implementing monitoring and filtering is not the only consideration, with views that Prevent contravenes academic freedom and freedom of speech (Cram and Fenwick, 2018). The Counter Terrorism and Security Act (2015) explicitly states that there must be particular regard to upholding freedom of speech and academic freedom, however this is still met with cynicism (Durodie, 2016). In addition, Sukarieh and Tannock (2016) postulate that Prevent can inhibit the ability to fully commit to research, which would be further enhanced by avoiding radical exploration of sensitive topic areas. If monitoring and filtering were implemented there is concern that development of thinking outside of the classroom will be inhibited (Cornell, 2016). Although a concern for universities, realistically filtering content would not necessarily stop sensitive research as academic material is still available on the internet (Terrazas-Arellanes et al, 2016), thus, the ability to find information will not be lost.

Methodology

Participants

In gathering views of specialists in Prevent and HE, semi-structured interviews were designed to assess how Prevent might be applied to cyberspace at universities. 26 Prevent designated leads were contacted via email to invite them and colleagues working in Prevent to take part in the study, selected simply by availability of information online. In addition two other individuals who work in Prevent and countering violent extremism were approached to take part in the study based on their input at a conference. One individual presented on perceptions of Prevent in education, and the second discussed how terrorist organisations are using social media to communicate with young people; both individuals participated in the study. Of the 26, three HE institutions took part in the study, three stated that they were unable to help with the research and there was no response from the further 20. Overall 16 individuals were interviewed for the study. Participants carried out a number of job functions, all involved in Prevent. Aside from the two individuals who took part due to their conference

input, each participant was a member of their university Prevent compliance board and therefore had a direct contribution to how their institution implements Prevent. Specific Prevent-based responsibilities of participants included delivering Prevent training to university staff, exploring implementation of monitoring and filtering, and directly engaging with students about Prevent. Participants carried out a number of job functions, all involved in Prevent. The sample was made up of Prevent designated leads (*N*=3), academics (*N*=3), university support staff (*N*=4), trade union representatives (*N*=1), university senior executives (*N*=1), SU staff managers (*N*=2), UK Government department Prevent advisors (*N*=1) and counter-narrative project officers (*N*=1).

Research limitations

The use of semi-structured interviews comes with limitations in that the data cannot be ground to fact, but instead are based upon individual experiences. It is therefore difficult to verify the provenance of an opinion, or whether it is informed. Qualitative research traditionally generates large amounts of data, and what is deemed significant can vary depending on the researcher, in particular where coding and analysis is done manually by one individual (Burnard, 1991). This could lead to exclusion of data that other researchers may perceive to be important. Nonetheless, capturing opinions and ideas from practitioners can help to inform development of operational practices, and contribute to the available research in a subject area (Barratt et al, 2011). In addition to the research conclusions being based on experiences and opinions, it has to be considered that, in the present study, there was input from relatively few participants. In this instance, however, limited responses from 26 contacted institutions reduced the potential participant pool.

Procedure

The present research received ethical approval by the corresponding author's institution research and ethics committee. Post approval, university designated Prevent leads were contacted to take part in the study. Initial information provided to individuals included

what the research sought to achieve, the nature of the interview and how the information provided would be used for the study. Those contacted were made aware that their identities, contributions and institution would remain anonymous. After informed consent was obtained from individuals to take part in the study, semi-structured interviews were designed to include topics to cover rather than a specific question set. The interviews were designed to be more 'conversational' than structured to improve the steady flow of discussion in a relaxed environment (Cerekovic et al, 2017). The 'conversational' approach concentrated on participants' views and experiences shaping the research outcomes, allowing themes and ideas to develop as the research unfolded. Topics planned to be included in the interviews were: participant knowledge of Prevent, social media and terrorism, Prevent in cyberspace, monitoring and filtering, alternative methods of applying Prevent in cyberspace, and future directions for Prevent. The initial discussion topics were available for participants to obtain on request. The interviews were conducted face-to-face at a convenient time for participants. Each interview was voice recorded and transcribed ahead of the thematic analysis. To maintain anonymity and distinguish between individual responses within the discussion, participants were assigned a code, from P1 to P16.

Data analysis

Each of the 16 interviews ranged from 20 to 50 minutes (M= 30.38 minutes, SD= 6.17 minutes), totaling in approximately 7.5 hours of data. Following the six steps outlined by Braun and Clarke (2006) a thematic analysis was conducted. Common themes were identified within the data set by familiarising and analysing each interview transcript (Braun and Clarke, 2006). Themes were identified through the initial codes and ordered into categories. Each of the categories were defined and further organised as to whether or not they aligned with the research objectives. Through this process it was clear which themes coincided with the problem the research sought to address, and how the categorised data set could be organised to form the basis of the discussion.

Results

The thematic analysis identified 27 themes within the interview data. The themes identified were organised into five categories: academic freedom, monitoring and filtering, responsibility of control and social media, influences outside of cyberspace, and counter-narratives. Participant responses on these themes are outlined in the discussion, and considered against the research objectives to directly inform the conclusions and recommendations of the study.

Discussion

Academic freedom

Academic freedom is considered as having free space to be able to research and discuss any topics within an educational boundary to find out information that is not yet known (Davies, 2015). Academic freedom is a core principle of a university and some participants in the present study stated it could be infringed with elements that Prevent has introduced to the HE sector:

> *A lot of academics are very negative about the whole Prevent agenda and while they might see what we are doing here at the moment as unproblematic they also think well it's only unproblematic at the moment and it is going to be ramped up so that it is going to deny people freedom of speech and freedom of opinion.* (P10).

Some participant academics spoke about potential implications of implementing monitoring and filtering. Particular concerns lied with researching topics that may be considered sensitive because of the belief that exploring information online, even if for the purposes of research could contravene Prevent and result in a referral to the police:

> *It would affect my research because if key words were triggered there would be people all over it. I don't know how it would affect it actually. It might inhibit people from being inquisitive. I think part of the tension with the Prevent duty is that you have a requirement as an education professional. As an education professional in Higher Education work or in schools you have on the one hand a requirement to provide opportunity to explore ideas to explore extreme ideas and they are learning, developing and playing with ideas.* (P12).

P12 discussed how Prevent could affect university research and could remove difficult but stimulating conversations from the education environment. Conversely the Counter Terrorism and Security Act (2015) specifically states that each university must have 'particular regard to the importance of academic freedom' in order to protect research in sensitive areas. Although the legislation provides a safety net for academic research, some academics are not wholly sold on the idea of Prevent, as one participant stated:

> *I think a lot of researchers and a lot of academics who work in areas that could be sensitive are nervous about putting certain words into search engines, often we self-censor ourselves before we realise we have even done it and I think we want to stay away from certain subjects and I think people who are really at the cutting edge looking at these issues, I think they would be very anxious and they would be wise to keep a wary eye.* (P8).

P8 discussed that people can sometimes sensor themselves subconsciously which can lead to being anxious about looking at sensitive areas, even for a research purpose. Some academics in the present study discussed the fear of the government 'knocking on your door' (P8) after typing things into search engines to which they relay to students within lectures on certain modules. Cynicism of Prevent was high in respect of constraining academic research,

however there was no evidence to suggest Prevent has impacted exploration of ideas or research. Instead, it could be considered that perceptions of Prevent are more of a barrier to research than Prevent itself. Universities are a safe space for students and academics to explore ideas and according to most participants Prevent allows that to continue. The line between expressing extremist views and researching an area, and the balance between protecting students from radicalisation and researching sensitive topics appears to be undefined. Some participants held the perception that Prevent and extremism research cannot coexist but as Prevent develops the resistance from academics towards Prevent may decrease and research could help to inform and assist HE institutions to implement the duty.

Monitoring and Filtering

Monitoring and filtering were discussed as implementation options by all participants in the present study. Some participants considered the link between filtering and radicalisation tenuous, and reflected on the realistic capability of implementing monitoring at universities. P7 stated, 'I can't believe there is a capacity to exist to watch every conversation … that is massive'. At a time when many students have personal devices that can connect to the internet via 3G and 4G networks, they are able to circumvent university Wi-Fi connections to access information on the open source web. P15 believed this was a barrier to implementing Prevent in cyberspace:

> *It's like having two bridges across the river and you shut the one bridge and you just walk across the other one … what can you do? That is technology and it is down to the government.* (P15).

In addition, P16 described any implementation of monitoring and filtering as a 'method to make it look like we are doing something' and was reluctant to suggest that there was a direct link between the methods and radicalisation. Where implementing an action simply to comply with the duty, as alluded to by P16, one has to question whether universities are taking the

duty to reduce risk of radicalisation seriously. Despite this factor, consideration has to be given to the skillset of a university to realistically identify students, or staff, at risk of being radicalised:

> *The public are not trained police officers and when I have this discussion with the police, we are doing what we can here, these are school teachers, these are gardeners, these are kitchen staff, these are wellbeing staff, you know, we are not trained police officers; we are doing what we can.* (P8).

Consideration of implementing monitoring and filtering therefore must go beyond the technical solution and instead contemplate the abilities of a university to evaluate such measures. P7 discussed that implementing the methods may cause more problems than solutions:

> *If you start monitoring and someone has looked at something that could lead to a right old industry on who are my officers to investigate, what do we do about it anyway, is it our business? Who are we to judge?* (P7).

Although monitoring can be seen as a deterrent (Loughry and Tosi, 2008), it was met with resistance by some participants. P9 suggested that monitoring could be seen as a breach of privacy:

> *It's a real challenging one, but then there is the flip side which is we have to, we do have a duty under Prevent to be reporting against any students who feel they are at risk and at the moment that is completely unchartered, we don't know what is going on in that space and we may think we are doing it brilliantly but actually when student 'A' comes into their halls of residence and looks at things on their*

> *iPad we don't know what is happening and it's about finding the balance and doing it the appropriate way.* (P9).

P9 discussed the challenging balance of identifying issues in cyberspace and encroaching on privacy. P9 also considered that students can use other networks to access the information which could possibly make monitoring difficult to identify undesirable online activity through the university servers. When students can use alternative methods to access content, the benefits of introducing monitoring and filtering in HE have to be questioned, and consideration must be given to control outside of HE.

Responsibility of control: adding social media into the mix

Participants in the study did not feel it was a university role to attempt to control the online space, for the reasons that it was not in the university skill set, and was a wider problem to regulate. P5 considered the intentions of monitoring and filtering on a scale wider than education:

> *The way cyberspace operates, it can be used by two individuals to communicate with information, news and beliefs and intentions to act. I think it's beyond any agency to control. Cyberspace is not controllable, it's not manageable, it's not as far as I can see, GCHQ may give you a different story, but as far as I can see it's not controllable. You can't stop two individuals using it to communicate in a way that creates a risk of extremist behaviour.* (P5).

P5 discussed potential difficulties for 'any agency' to control cyberspace. In addition, P13 identified social media as a barrier to the ability to control the internet, 'social media is just, you can't stop it, you know, if you do people will just find another way around it'. Due to the confines of freedom of speech it could be considered unethical to monitor student's social

media activity, as Ceron and Memoli (2016) describe social media to be a key form of democracy in today's society. With mass access to cyberspace within society the ability to control every aspect of it can be difficult. As technology develops further it could create more avenues available for terrorist organisations to communicate, enhancing the challenge to extremist content online both for and outside of the HE sector:

> *We can contact each other, Skype each other, get books off Amazon etc, watch Game of Thrones for free, we can do all of that and its brilliant, we love it. That's the very same freedom that allows terrorists to communicate with each other, allows terrorists to put up propaganda and allows terrorists to groom young vulnerable people and get them together and we can't have one without the other I'm afraid and we kind of know that and terrorism is always there as a kind of, as a virus in our system so … there's nothing we can really do about it and I don't think many of us trust nation states to trust people to stop it.* (P8).

P8 described that the ability to communicate in cyberspace can potentially create problems, as well as advantages within society. Interconnectivity has been improved with the implementation and development of social media and as more companies develop messenger style apps, P10 suggests that monitoring conversations or having the ability to identify 'communications that are dangerous' becomes more challenging. Barber and King (2017) discussed that Westminster attacker Khalid Masood was in contact with others via WhatsApp minutes prior to the incident being carried out and the social media app has been criticised since. WhatsApp offers encrypted messages to avoid being seen as a part of a big brother style monitoring of communications. Terrorist organisations use many social media platforms but the encrypted messages that WhatsApp provide have come under scrutiny for not doing more to monitor criminal activity that is being planned and discussed within the confines of the app. With scrutiny toward large corporations for terrorist organisations using their platform, the concept of implementing cyberspace measures for Prevent in HE is daunting, and an issue for

the wider government. Although control of cyberspace appears difficult, the way in which authorities use it could be improved to help mitigate against terrorist use of cyberspace.

A popular facet of social media is the sharing of videos and vlogging, in particular via YouTube. Araujo et al (2015) postulate that providing information by video is far more likely to have an impact on the audience due to the visual aesthetics that can help trigger emotions. P14 used the example of Daesh propaganda videos stating that 'its slick, its sexy, its high quality, its cutting edge, they have a marketing department and they take this very seriously'. P2 stated 'maybe the authorities should use social media more effectively to counter some of the narrative that ISIS is putting out'. In addition, P13 discussed how important communication with the public can be:

> *We have so many vloggers and so many right wing, left wing speakers that and they are the people that UK public are listening to. They are the people that are engaging with the public, the groups that are advising the government, they aren't very good at engaging with the public.* (P13).

Universities could provide an opportunity, whereby students who understand the key communication tools available to young people could help to develop content which would assist informed communications on sensitive issues such as extremism. Utilising the knowledge base of universities and students could enhance compliance with Prevent, and work towards making a difference to countering extremism outside of HE.

Influences outside of cyberspace: playing to university strengths

Participants highlighted that Prevent discussions around cyberspace appear to focus solely on technological solutions and, instead, gave consideration to the factors driving extremism, with rationale explained by P16:

> *Radicalisation happens outside of cyberspace, I would say cyberspace provides a platform or space where radicalisation can take place but I think there have to be other factors that are going on, or other drivers which may cause someone to kind of move in that direction.* (P16).

Concentrating on influencing factors outside of cyberspace poses the question of why activity in a virtual space is treated differently from that in the real world. Using non-technological methods, applied to cyberspace, could be more suited to the skillset and knowledge of university staff and P2 discussed implementing Prevent into the curriculum:

> *I think educating our students is a huge challenge but also an opportunity for us, and I think an opportunity we aren't realising would be around building elements of Prevent and preventing violent extremism into relevant parts of the curriculum so it wasn't seen as an add on.* (P2).

As P2 postulates, having Prevent in the course so it is not an 'add on' will ensure students engage with Prevent, allowing discussions about difficult topics. P3 discussed that there are underlying factors to being radicalised which often have 'religious imagery but … it's ultimately, to some extent, reasonable political grievances.' Discussing Prevent in lectures allows the safe space to develop understanding of 'political grievances' and other ideology that can lead to radicalisation. This approach supports the research findings from Streitwieser et al (2019) who suggest that universities should 'encourage more learning opportunities … that directly address the problem of radicalisation.'

Where this concept is applied to cyberspace, the impact that the online space has on radicalisation of students could potentially be reduced. Prevent could be applied to cyberspace as a mechanism to increase resilience and educate individuals to challenge extremist ideology presented online. According to Zsidisin and Wagner (2010), the perceptions that people develop online can often become their reality. With respect to the perceptions formed by

young people, one response is through education, as noted by P2, who stated, 'I think the really important area where we can influence and make a really big difference [is in] educating young people'. Education can thus serve to counter the narratives of terrorist organisations, and be applied to cyberspace.

Building counter-narratives: an alternative solution?

Participants built on the education discussion by concentrating on the narratives available to combat extremism. P12 stated 'the only counter-narrative that Prevent offers us is a narrative of fundamental British values' which Curren (2017) argues should promote 'respect and tolerance' for cultural differences. One participant discussed how 'fundamental British values' links to radicalisation:

> *The notion of fundamental British values is problematic in its own right and so I think we are dealing with complexity, built on complexity built on complexity and when that meets in Higher Education, what have we got? We have a narrative of fundamental British values to counter a radicalisation agenda or a radicalisation narrative and that's insufficient I think because its insufficiently understood, it's insufficiently argued it's insufficiently engaged with by people, it's not a narrative that people regularly use, a narrative of fundamental British values is not a British narrative today.* (P12).

P12 discusses the problems associated with the fundamental British values narrative in that it is difficult to interpret what it means, in particular with regard to counter radicalisation. Elton-Chalcraft et al (2017) outline that a lack of understanding of what fundamental British values means leaves the concept unchallenged, which can create uncertainty about the premise of Prevent (Busher et al, 2017) through 'the way it stigmatises … Muslim communities in particular' (P3). Vanderbeck and Johnson (2016) suggest that the focus should be on building respect for cultural and religious differences, rather than on 'British values', which can have a

tendency to undermine the safeguarding purpose of Prevent (Coppock and McGovern, 2014). In support of this approach was P14:

> *I don't like using the term British values because it is restrictive but, in keeping with human values, so kind of tolerance, respect for everyone and they are pluralist values that I too I think, [can benefit] lots of different countries not just the UK.* (P14).

British values as a narrative could instead include other cultural beliefs to avoid perceived negative connotations of racism and targeting of student communities being associated with Prevent. Instead of Prevent concentrating on a non-established concept, it could be used as a platform to address grievances that lead to extremist behaviours and beliefs. Counter-narratives could then be created in education to address the specific grievances identified. P14 discussed a successful counter-narrative campaign:

> *Abdullah X was made by a former Islamist extremist and is a cartoon … I think it was after Charlie Hebdo. They put out animation talking about all of the grievances that those perpetrators had and there were people following Islamist ideology have but in a deconstructed way and in a way that was like, I have this grievance but I'm not going to go and shoot someone. It was trying to show the message that these grievances exist but violence is not the answer.* (P14).

Organisations such as ISD produce counter-narrative materials which can be shared on social media to provide effective information against extremist ideologies (Straw, 2016). ISD assist schools with Prevent by showing counter-narrative videos (Extreme Dialogue, 2017); a similar approach could be taken in HE. Producing counter-narratives might be considered a challenge for universities; however, using the student engagement requirement, and introducing Prevent into relevant courses, students could develop their own counter-narratives

specific to their university environment. Where embedded into the curriculum, Prevent could help to develop understanding of grievances and vulnerabilities that influence radicalisation in that geographical area. As an extension of the knowledge learnt, within a module, students could create counter-narrative content to be released on social media platforms to counter extremist arguments within cyberspace.

Conclusion

The present study has identified potential methods in which Prevent might be applied to cyberspace in HE. Initially this was done by assessing the ability of monitoring and filtering, both as methods that are required to be considered as per the Prevent Duty Guidance for HE (2015). By conducting 16 semi-structured interviews with individuals working in Prevent and HE consideration has been given to whether the methods can realistically tackle radicalisation in cyberspace at universities, and be supported by university staff.

Firstly, participants did not see the link between radicalisation and use of monitoring and filtering in HE, due to the limited capacity of the university network. The ability for students to use 3G and 4G networks to access the internet makes the monitored and filtered network too easy to circumvent, rendering the methods limited in the university environment. P16 stated that implementing monitoring and filtering would be a 'method to make it look like we are doing something', thus suggesting that support for implementation was limited. Other arguments against the methods were led by limiting ability to research sensitive topics, and infringement on academic freedom. Despite reassurances from the Counter Terrorism and Security Act (2015), some academics felt that 'it's only unproblematic at the moment and [Prevent] is going to be ramped up' (P10) which may encroach on academic exploration.

With reluctance to implement monitoring and filtering, participants considered applying non-technological methods to cyberspace. P2 believed 'Prevent and preventing violent extremism [should be embedded] into relevant parts of the curriculum' to improve the

ability of students to understand and challenge extremist narratives. To include Prevent into relevant courses would help meet student engagement compliance with the duty, and build a greater understanding of influencing factors that may lead someone to radicalisation. By learning about extremist ideology, within the confines of a module, participants suggested students would be better placed to notice changes in behaviour that might leave an individual vulnerable to a range of negative influences, including radicalisation. As part of a module, students could create counter-narrative content for cyberspace, to both meet Prevent compliance, and develop resources to help counter extremism both inside and outside of HE.

The present study thus offers several areas that universities might consider to implement Prevent in cyberspace. Firstly, monitoring and filtering should not be made a compulsory element of the Prevent duty, and it should be the discretion of individual universities on whether to implement these methods. Secondly, online implementation should be about addressing the drivers to radicalisation that occur in the offline space, and applying the concepts to cyberspace. This not only plays to university strengths of using education to build resilience and knowledge, but keeps the basis of Prevent more in line with the academic values of a university. Third, building Prevent into relevant parts of the curriculum should be considered by universities, in order to create resources to help address specific drivers to radicalisation within HE, and ultimately meet the student engagement compliance factor of Prevent.

Recommendations

In order to move the Prevent duty from one of compliance to a mechanism to make an effective contribution to countering violent extremism, universities should consider implementing a module to develop student knowledge of radicalisation. Universities could better understand the drivers that make individuals vulnerable to a range of negative influences, radicalisation being one. By understanding the drivers, safeguarding measures can be put in place to mitigate against the specific vulnerabilities associated with university students. Within the module, students could be educated to better understand how to challenge

information, helping them to build resilience to negative influences and to identify misinformation.

In applying the module to implementation of Prevent in cyberspace, student use and knowledge of social media could be utilised to think about the current methods of communication and how terrorist organisations might reach out to young people. The output of the module would be developing counter-narratives to specific radicalisation drivers identified by the university. Through developing counter-narrative content for the latest social media platforms, a bank of content could be produced to help challenge extremist narratives both in and outside of the education sector.

There are many benefits of taking this approach to implementing Prevent in cyberspace that fall outside of compliance with the duty. First, engaging students in discussions on challenging issues, and developing a greater understanding of drivers to becoming involved in undesirable activities. Second, by producing counter-narratives students will be creating products that will be able to showcase their skills, and therefore enhance their employability as a result. Third, by understanding the issues, students can begin to develop greater resilience to negative influences and better challenge information.

References

Abdulhamid, S and Ibrahim, F, 2014. Controlling citizens cyber viewing using enhanced internet content filters *Information Technology and Computer Science,* 12 (1), 56-63

Acik, N., Deakin, H and Hindle, R, 2018. Safeguarding, surveillance and control: school policy and practice responses to the Prevent duty in the 'war on terror' in the UK, *The Palgrave International Handbook of School Discipline, Surveillance, and Social Control,* 467-489

Aloi, G., Di Felice, M., Loscri, V., Pace, P and Ruggeri, G, 2014. Spontaneous smartphone networks as user-centric solution for the future internet, *Communications Magazine,* 52 (12), 26-33

Araujo, T., Neijens, P and Vliegenthart, 2015. What motivates consumers to retweet brand content? The impact of information, emotion and traceability on pass-along behaviour, *Journal of Advertising Research,* 55 (3), 284-295

Awan, I, 2017. Cyber extremism: ISIS and the power of social media, *Society,* 54 (2), 138

Barber, N and King, J, 2017. Henry Pearce: some thought on the encryption regulatory debate, *UK Constitutional Law Association,* 4 (25), 8-15

Barratt, M., Choi, T and Li, M, 2011. Qualitative case studies in operations management: trends, research outcomes, and future research implications, *Journal of Operations Management,* 29 (4), 329-342

Bertram, L, 2016. Terrorism, the internet and the social media advantage: exploring how terrorist organisations exploit aspects of the internet , social media and how these same platforms could be used to counter violent extremism, *Journal for Deradicalisation,* 7 (1), 225-252

Braun, V and Clarke, V, 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology,* 3, 77-101

Burnard, P, 1991. A method of analysing interview transcripts in qualitative research, *Nurse Education Today,* 11 (6), 461-446

Busher, J., Choudhury, T., Thomas, P and Harris, G (2017). *What the Prevent duty means for schools and colleges in England: An analysis of educationalists' experiences.* Research Report. Aziz Foundation

Cerekovic, A., Aran, O and Gatica-Perez, 2017. Rapport with virtual agents: what do human social cues and personalities explain?, *Transactions on Affective Computering,* 8 (3), 382-395

Ceron, A and Memoli, V, 2016. Flames and debates: do social media affect satisfaction with democracy?, *Social Indicators Research,* 126 (1), 255-240

Considine, B., Krahel, J., Lenk, M and Janvrin, D, 2016. Social technology: a compendium of short cases, *Issues in Accounting Education,* 31 (4), 417-430

Coppock, V and McGovern, 2014. 'Dangerous minds'? Deconstructing counter terrorism discourse, radicalisation and the 'psychological vulnerability' of Muslim children and young people in Britain, *Children and Society,* 28 (3), 242-256

Cornell, H, 2016. Counter terrorism, radicalisation, and the university: debating the Prevent Strategy, *Global Justice Academy Blog,* 1 (20), 9-15

Costa, D, 2015. First word, *PC Magazine,* 1 (1), 6-8

Counter Terrorism and Security Act (2015). Available at http://www.legislation.gov.uk/ukpga/2015/6/pdfs/ukpga_20150006_en.pdf (Accessed: 7th November 2016)

Cozine, K, 2016. Social media and the globalisation of Sicarii, *Global Security Studies,* 7 (1), 1-12

Cram, I and Fenwick, H, 2018. Protecting free speech and academic freedom in universities, *Modern Law Review,* 81 (5), 825-873

Curren, R, 2017. Why character education?, *Impact,* 24 (1), 1-44

Davies, M, 2015. Academic freedom: a lawyer's perspective, *The International Journal of Higher Education Research,* 70 (6), 987-1002

Durodie, B, 2016. Securitising education to prevent terrorism or losing direction?, *British Journal of Educational Studies,* 64 (1), 21-35

Elton-Chalcraft, S., Lander, V., Revell, L., Warner, D and Whitworth, L, 2017. To promote, or not to promote fundamental British values? Teachers' standards, diversity and teacher education, *British Educational Research Journal,* 43 (1), 29-48

Extreme Dialogue (2017). About Extreme Dialogue, Available at http://extremedialogue.org/about/ (Accessed: 15th March 2017)

Goodman, S., Kirk, J and Kirk, M, 2007. Cyberspace as a medium for terrorists, *Terrorism and Technology, Technological Forecasting and Social Change,* 74 (2), 193-210

Guiora, L, 2018. Inciting terrorism on the internet: the limits of tolerating intolerance, *Incitement to Terrorism,* 253 (1), 1-10

Hare, C, 2017. Digital surveillance detrimental to learning, expert says, *ATA News,* 51 (10), 12-13

Heath-Kelly, C and Strausz, E, 2018. The banality of counterterrorism 'after, after 9/11'? perspectives on the Prevent duty from the UK health care sector, *Critical Studies on Terrorism,* DOI: 10.1080/17539153.2018.1494123

Institute for Strategic Dialogue (2019). Innovation Fund Round 1 Awarded Projects, Available at https://www.isdglobal.org/innovation-fund/innovation-fund-round-1/ (Accessed: 14th April 2019)

Isaacson, S, 2016. Finding something more in targeted cyberspace activities, *Rutgers University Law Review,* 68 (1), 905

Lee, P., Hui, S and Fong, A, 2005. An intelligent categorisation for bilingual web content filtering, *Transactions on Multimedia,* 7 (6), 1183-1190

Loughry, M and Tosi, H, 2008. Performance implications of peer monitoring, *Organisation Science,* 19 (6), 876-890

McNicol, S, 2016. Responding to concerns about online radicalisation in UK schools through a radicalisation critical digital literacy approach, *Computers in the Schools,* 33 (4), 227-238

McQueeney, K, 2014. Disrupting Islamophobia: teaching the social construction of terrorism in the mass media, *International Journal of Teaching and Learning in Higher Education,* 26 (2), 297-309

Miah, S, 2017. The Prevent policy and the values discourse: Muslims and radical governmentality, *Muslim Students, Education and Neoliberalism: Schooling a 'suspect community',* 1 (1), 131-144

NUS (2015). Preventing Prevent handbook. Available at http://www.nusconnect.org.uk/articles/preventing-prevent-handbooks (Accessed: 20th March 2017)

O'Connor, K., Schmidt, G and Drouin, M, 2016. Suspended because of social media? Students' knowledge and opinions of university social media policies and practices, *Computers in Human Behaviour,* 65 (6), 619-626

Pal. S, 2015. Spies, surveillance and stakeouts: Monitoring Muslim moves in British State Schools, *Race, Ethnicity and Education,* 18 (2), 183-201

Prevent Duty Guidance for Higher Education Institutions in England and Wales (2015). Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf (Accessed: 12th March 2017)

Prevent Duty Guidance for Higher Education Institutions in Scotland (2015). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445921/Prevent_Duty_Guidance_For_Higher_Education__Scotland_-Interactive.pdf (Accessed: 20th November 2017)

Ribeiro, J, 2015. Facebook to widen use of safety check tool beyond Paris attacks, *PC World,* 1 (1), 1

Santoro, D, 2018. A cosmopolitanism of fear: the global significance of terrorism after 9/11, *Knowledge Cultures,* 6 (3), 28-42

Straw, W, 2016. How do you get people to leave Islamist or neo-nazi movements?, *Left foot forward: Evidence Based Political Blogging,* 8 (5), 36-45

Streitwieser, B., Kristen, A., & Duffy-Jaeger, K, 2019. Higher Education in an Era of Violent Extremism: Exploring Tensions Between National Security and Academic Freedom. *JD Journal for Deradicalisation, Spring 2019* (18), 74-107

Sukarieh, M and Tannock, S, 2016. The deradicalisation of education: terror, youth and the assault on learning, *Race and Class,* 57 (4), 22-38

Terrazas-Arellanes, F., Knox, C., Anderson-Inman, L., Walden, D and Hildreth, 2016. The SOAR strategies for online academic research, *Special and Gifted Education,* 1 (1), 351-389

Theohary, C and Rollins, J, 2011. Terrorist use of the internet: information operations in cyberspace, *International Journal of Terrorism and Political Hot Spots*, 6 (4), 597-614

Thorne, A, 2015. Social media, civility and free expression, *Academic Questions*, 28 (3), 334-338

Vanderbeck, R and Johnson, P, 2016. The promotion of British values: sexual orientation equality, religion, and English schools, *International Journal of Law, Policy and the Family*, 30 (3), 292-321

Weimann, G (2014). *New Terrorism and New Media*. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars

Wolff, J and Lehr, W, 2018. When cyber threats loom, what can state and local governments do?, *Georgetown Journal of International Affairs*, 19 (1), 76-82

Wright, J and Breindl, Y, 2013. Internet filtering trends in liberal democracies: French and German regulatory debates, *Internet Policy Review*, 2 (2), 1

Xie, Y., Qiao, R., Shao, G and Chen, H, 2016. Research on Chinese social media users' communications during public emergency events, *Special Issue on Social Media in China, Telematics and Informatics*, 34 (3), 740-754

Zelenkauskaite, A and Balduccini, M, 2017. 'Information warfare' and online news commenting: analysing forces of social influence through location based commenting user typology, *Social Media and Society*, 3 (3), 1-13

Zsidisin, G and Wagner, S, 2010. Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence, *Journal of Business Logistics*, 31 (2), 1-20

Zucker, A, 2019. Using critical thinking to counter misinformation, *Science Scope*, 42 (8), 6-9

About the JD Journal for Deradicalization

The JD Journal for Deradicalization is the world's only peer reviewed periodical for the theory and practice of deradicalization with a wide international audience. Named an "essential journal of our times" (Cheryl LaGuardia, Harvard University) the JD's editorial board of expert advisors includes some of the most renowned scholars in the field of deradicalization studies, such as Prof. Dr. John G. Horgan (Georgia State University); Prof. Dr. Tore Bjørgo (Norwegian Police University College); Prof. Dr. Mark Dechesne (Leiden University); Prof. Dr. Cynthia Miller-Idriss (American University Washington); Prof. Dr. Julie Chernov Hwang (Goucher College); Prof. Dr. Marco Lombardi, (Università Cattolica del Sacro Cuore Milano); Dr. Paul Jackson (University of Northampton); Professor Michael Freeden, (University of Nottingham); Professor Hamed El-Sa'id (Manchester Metropolitan University); Prof. Sadeq Rahimi (University of Saskatchewan, Harvard Medical School), Dr. Omar Ashour (University of Exeter), Prof. Neil Ferguson (Liverpool Hope University), Prof. Sarah Marsden (Lancaster University), Dr. Kurt Braddock (Pennsylvania State University), Dr. Michael J. Williams (Georgia State University), and Dr. Aaron Y. Zelin (Washington Institute for Near East Policy), Prof. Dr. Adrian Cherney (University of Queensland).

For more information please see: www.journal-derad.com

Twitter: @JD_JournalDerad
Facebook: www.facebook.com/deradicalisation

The JD Journal for Deradicalization is a proud member of the Directory of Open Access Journals (DOAJ).

ISSN: 2363-9849

Editor in Chief: Daniel Koehler