THE UNIVERSITY OF HULL

Department of Criminology and Sociology

Analysing the Threat from Cyber-extremism in the Humberside Policing Area

Being a dissertation submitted in partial fulfilment of the requirements for the degree of Master of Arts Criminal Justice and Crime Control

October 2021

Neil Kitching, BA hons

Acknowledgments

I would like to thank all the faculty from the Department of Criminology and Sociology for their professionalism and their ability to adapt considering the challenges forced upon them from the COVID-19 pandemic. A particular thank you goes to Dr Denise Carter, my supervisor for this module, who is also the only faculty member I had the chance to meet face to face. Her knowledge and wisdom an ever comfort when juggling my academic studies with my role in Counter Terrorism policing. Lastly, I would like to thank my wife and my two girls for putting up with me and graciously sharing our time with my studies.

Abstract

This dissertation details a study that was conducted in the Humberside policing area with the aim of determining the current threat from cyber extremism to 16 to 18 year olds in further education is. Counter Terrorism policing has had to adapt to the ever-changing landscape associated to extremist material posted onto the internet. And this study focuses on identifying what the risk is at a micro level rather than a hypothetical national macro level. The results confirming a hypothesis that the internet being universal enables the extremist to scatter gun extremist and hatred material online with very little chance of identification. Their ambition is to indirectly radicalise a vulnerable person and potential inspire them to commit a violent extremist act or radicalise others themselves.

The study also details what social media platforms are being used and some of the extremist material seen by young people and how they felt about what they had seen whether they are likely to report concerning material and if so, who would they choose to report it to.

The study when exploring extremism was faced with a question as to whether the Incel sub-culture is an extremist ideology or not and discusses the current Counter Terrorism response considering the media reporting to the aftermath of the Plymouth murders at the hand of Jake Davison, a self-identified Incel.

Thew study concludes by introducing the authors professional observations as a Counter Terrorism officer and combines them with the study's findings to offer a working hypothesis that the internet is distorting vulnerable people's perception of life which in turn causes unnecessary strain which can manifest into anomie and no mobilisation of a self-initiated terrorist.

Contents

Chapter 1 - Introduction

Principally this dissertation is an investigation into understanding the current threat from cyber extremism in the Humberside Policing area by way of qualitative study conducted with students aged between 16 to 18 years old who are attending further education colleges; however to provide some context, the research was conducted by a serving Counter Terrorism Police Officer working in PREVENT (Chapter 2) which added another layer of complexity to the study as many of the gatekeeper issues were resolved by the subjects already established professional relationships with the colleges and other pertinent partners. Therefore, to explain this relationship in more detail the first chapter of this dissertation is devoted to providing a background into Counter Terrorism, the structure of modern Counter Terrorism, the introduction of the CONTEST strategy and later a particular focus on PREVENT, the legal duty it imposes, and the Channel panel. As well as adding to academic writing the study was of interest to the four local authority Multi-Agency Partnership boards (Chapter 2) responsible for the study's geographical area and is likely to better guide them on mitigating risk from cyber inspired extremism.

Whereas it is accepted that the internet and its content is universal and therefore from a macro level any research into threat, risk and harm can be established by utilising a wide range of researching methods for example cyber ethnography (Eichhorn, 2001) This study looks at threat, risk, and harm on a micro level and in a geographical area that is largely unaffected by other forms of extremist influence. The study therefore comes from a perspective that any extremist activity in the geographical area is highly likely to come from a cyber source as opposed to a physical person who could be described as a radicaliser.

Counter Terrorism in the UK has seen the evolution of terrorism and extremism and watched as it progressed into the cyber age. An age where the reach of an extremist and their ability to radicalise and inspire another to commit a violent extremist act even though they had never met has sent shockwaves through society that resonates today. Since the fall of the Islamic state there has still been several terrorist related attacks committed in their name or ideology. Later investigations had shown that the offenders who had either chosen not to travel, or whose travel had been frustrated by security services, none of them would have received face to face instructions or direction on how to commit the act they did. The inference being they were highly likely radicalised and obtained knowledge on how to commit their atrocities from a cyber source instead. Furthermore, there has been an increase and an aspirational adopting of methodologies from Islamic state and other religiously extreme groups by right wing extremist groups resulting in many arrests of potential terrorist from this thematic. Again, where the radicalisation and inspiration to commit an act is likely to be linked to a cyber source.

Chapter 3 details the study with the aim of answering three broad questions: -

What are the current trends related to young people's cyber usage in the Humberside policing area?

What extremist/hate material have young people in the Humberside policing area been exposed to?

How confident are young people in reporting concerning matters/material they have seen on the internet?

The latter question is vitally important and challenges any perception as to whether the Counter Terrorism policing and its partners can consider themselves as effectively mitigating the current threat or falling into a trap of only being concerned with what they know. The British public quite rightly after a terrorist related incident will ask whether there was anything that could have been done to stop it. It would be indefensible to maintain a position that no one knew that an individual had a desire to commit an act or was being exposed to extremist material because they were not referred for support. Therefore, Counter Terrorism should apply equal weight to creating an environment where the public feels confident and easily knows how to refer a vulnerable person alongside directly supporting those that have been referred.

The study is not designed to seek out future offenders or to support a potential police investigation into individuals, but rather to understand how likely a young person is to come across extremist/hate material on the internet as well as the likelihood of them being contacted directly. From the authors own experience of being directly involved with those that have been identified as being vulnerable to radicalisation it can be commented that there are several reasons why someone may become vulnerable and not all vulnerable individuals will pose a threat of committing a violent extremist act. The identification of these vulnerabilities is not in the scope of this study but are referred to and compliment the conclusion (Chapter 5).

An unexpected outcome from the study has given some validity to exploring a new and emerging sub-culture that closely mirrors extremism and radicalisation but currently is not considered an extremist ideology by UK Counter Terrorism Policing. Inceldom has been borne from the internet firstly in North America but has since made its way over to the UK. Chapter 4 details Inceldom, their belief system and how such a system can draw someone into committing a violent act in a very similar manner to an extremist. The chapter also details the current police response and how PREVENT is at the forefront of mitigating the threat, risk and harm associated.

Chapter 2 - Counter Terrorism Policing in the UK

The purpose of this chapter is to give some context on the position the study's author is in. The study's assumption is that many researchers into the causes and effects of terrorism are going to be academics with very few with actual experience of working within Counter Terrorism or being employed by a governmental agency. It is probable that their findings will come with security classifications and is not readily available to most people. This dissertation bridges this by providing some non-sensitive insight into the procedures associated to preventing extremism and individuals becoming terrorist. To do this the chapter is split into two contextual areas. The first covers a brief history of Counter Terrorism in the UK, the structure, and the formulation of the UK's current response to threat of terrorism referred to as CONTEST. The second is a more detailed look at the PREVENT strategy of CONTEST, the legislation underpinning the strategy, and the Channel panel which is the safeguarding panel charged with supporting and de-radicalising where necessary individuals identified as being vulnerable to radicalisation.

2.1 The CONTEST strategy

Counter Terrorism within the UK can be arguably split into two zeitgeists, namely pre and post 9/11 coupled with the London bombings in 2005. Before these two significant historical events Counter Terrorisms in the UK was conducted at a Police Constabulary level and mainly focused on the then identified threat from Northern Irish related terrorism and supporting counter espionage activities. These legacy policing units were referred to as 'Special Branch' and were formed in 1883 sharing a direct lineage with the Special Irish Branch (SIB). Post World War II, both the Security Service (MI5) and the Secret Intelligence Service (MI6) had been structured to respond to the 'Cold War', the monitoring of the former Soviet Union and in respect of MI6 providing support to counter insurgency in the former British colonies.

After the Twin Towers terrorist attack in New York on the 9th of September 2001 the UK government understood that the face of terrorism had changed and reviewed their response with a greater emphasis of understanding and mitigating the then overwhelming threat from religious extremism connected to Al-Qaeda. In 2003 the UK governments designed their first comprehensive counter-terrorism strategy, known as CONTEST (House of Commons Home Affairs Committee, 2009). CONTEST outlined four distinct thematic areas commonly referred by counter terrorism practitioners as the four P's. PREVENT, to stop people becoming terrorists or supporting terrorism and covered in chapter 2. PURSUE, to stop terrorist attacks. PROTECT, to strengthen our protection against a terrorist attack. PREPARE, to mitigate the impact of a terrorist attack (HM Government, 2018). This strategy manly relies on two definitions, terrorism, and extremism to gain a mandate for its activities.

Terrorism is defined as the use or threat of action, both in and outside of the UK, designed to influence any international government organisation or to intimidate the public. It must also be for the purpose of advancing a political, religious, racial, or ideological cause. Terrorist related activity have always been considered a criminal offence and therefore its definition is enshrined in UK law and enforced like much the same as all other laws by UK police. The second definition, extremism appears to have been borne to give PREVENT a mandate where no criminal offence has been committed but gives justification for UK police officers to operate where, there is reasonable suspicion that a vulnerable person is being exposed to or being inspired by extremism, consequentially this has been met with a wave of criticism from some quarters (Walker & Cawley, 2020). Some academics have argued that using terms like extremism comes with some inherent problems and at first sight, one might say that such a semantic view is useless in searching for a proper definition of the term extremism (Sotlar, 2004). Despite this observation the UK government has defined extremism as the vocal or active opposition to our fundamental values including, democracy, the rule of law, individual liberty and respect and tolerance for different faiths and beliefs. It also regards calling for the death of members of the armed forces as extremist behaviour (HM Governemnt, 2015). In defining extremism, the UK Government appears to have applied normative ethics and have opted for an absolutist approach by outlining one set of ethical standards that applies across all societies (Banks, 2016). However, when the definition was first published there were many who challenged the governments approach. This has likely spurned some of the negativity towards PREVENT, especially over the argument as to whether there should be a redaction of the word 'British' in the definition when highlighting values. Critics of the definition may come from a position that the government has ignored ethical relativism and what is morally right or wrong may vary in a fundamental way from person to person or from culture to culture (Banks, 2016). Also, the definition appears to be vague, and the lack of detailed guidance can easily allow the misinterpretation of the definition and give an opportunity or cause net-widening to occur without careful governance from government and society (Blomberg & Mastre, 2014). Furthermore, the definition makes very little distinction between violent and non-violent forms of extremism which can and likely causes confusion to those that have a duty to refer vulnerable people as to when it is appropriate to do so. Consequently, causing several embarrassing examples of very young children to be referred to Counter Terrorism without having first gaining some basic context to what was being espoused where later exploration showed there was no indication that the child was vulnerable to radicalisation.

2.2   PREVENT and Channel

Of all the sub-strategies associated to the CONTEST strategy PREVENT has been the most contentious and there has been many calls for it to be abolished, citing it as being Islamophobic (Cohen & Tufail,

2017) (Younis & Jadhav, 2019) (Ghani & Nagdee, 2019). At the time of writing this dissertation PREVENT is undergoing an independent review to determine if the government strategy for supporting people vulnerable to being drawn into terrorism is effective and whether there is a necessity to modify or abandon the strategy all together. The author is a Counter Terrorism Case Officer, formerly referred to as either a PREVENT Officer or Channel Officer and it is with this insight of the inner workings of a Channel and the dynamics that effect Channel that this section is built upon.

In 2015 the UK government introduced the Counter Terrorism and Security Act which placed a duty on selected government agencies, education providers, and health trusts to prevent those from being drawn into terrorism. Behind the scenes there was a handing over of the responsibility from policing to the local authority for the management and leadership of how PREVENT is delivered locally from a strategic standpoint, what was introduced was the Multi-Agency Partnerships. The Multi-Agency Partnership boards consist of senior leaders from local government, educational and health sectors whose role is to create and implement PREVENT delivery plans. These consist of an engagement strategy, support for individual agencies training plans and governance to the Channel panel. They also receive, acknowledge, and devise a plan to mitigate the identified risk detailed in the Counter Terrorism Local Profile or CTLP (HM Governemnt, 2012). These local profiles form the foundation for all activity, provides direction and gives a mandate to deploy appropriate resources. The CTLP carries a UK governmental classification of 'Official Sensitive' but in a 'Non-Protectively Marked' version is also produced which some local authorities choose to publish on their websites. The resulting activities of the PREVENT are likely to be unnoticed as they become integrated into other initiatives lead by the local authority; however, one area that has gained some media attention is the prohibition of certain speakers in universities. These speakers having been linked to extremism were forbidden a platform to either debate or share their views. A position criticised by some who believed that the universities should not be coerced either by legislation or by an outside governing body (McGovern, 2016).

The Channel panel is a non-judgemental paternalistic safeguarding panel which seeks justification and aims to defend relatively helpless or vulnerable people from external dangers namely, radicalisation and the harm it causes from individuals, groups or institutions associated with extremism when the protected parties are not voluntarily consented to the risk (Feinberg, 1989); however it always seeks to gain consent for any support package. The panel is lead, administered, and governed by the relevant local authority. Its membership can be different from one panel to the next, but it is highly likely that many of the standing memberships will be from agencies listed in Schedule 6 of the Counter Terrorism and Security Act '2015 including social workers, health professionals and both Counter Terrorism and

constabulary police officers or staff to list a few. Since the information being discussed is sensitive, all members must agree to a confidentiality clause before the panel; however, this does create a form of a professional induced echo chamber and the panel becomes incredibly reliant on the knowledge and understanding of the radicalisation process by its members to be effective. Poignantly depending on the wealth and how a local authority is funded it is likely that the Counter Terrorism Case Officer is the only panel member working in this thematic full time and the only member who has had the opportunity to develop their knowledge on the subject thus becoming a subject matter expert. Furthermore, it is likely that most cases are put before the panel after an initial assessment has been made by the Counter Terrorism Case Officer. This can wrongly give the impression that even though the chair of the panel is a local authority officer, Counter Terrorism Policing are still very much in control of what happens at the panel. This is likely not to be what was intended when they were structured, especially if there were a disagreement of opinion which would require a panel member to have the strength of character to challenge and put an alternative view against that of a subject matter expert and be able to rally enough support from other panel members to go on record against the advice being offered.

Principally the panel has two broad methodologies to support a person deemed vulnerable to radicalisation. The first is to identify the sociological causes that led to someone becoming vulnerable to radicalisation. This can be a mixture of static vulnerabilities and those that are able to be mitigated. Examples of static vulnerabilities maybe their age, past experiences, and mental health concerns to name a few. Whereas these can be supported, and assistance given with the management of these vulnerabilities, the fact is they have an element of permanence or in the very least a vulnerability that will be with the person for some considerable time. Examples of vulnerabilities that can be mitigated are employment, education, and access to housing, again to name a few. This first area calls for the expertise of several professionals that can offer services and make decisions on behalf of those services to mitigate where they can.

The second methodology used by the Channel panel is the suppression or the supplying of counter narrative to the ideology linked to the subject. It is advocated that the latter is completed by an accredited person referred to as a Home Office Intervention Provider. The accreditation and management of these providers is done by newly rebranded Homeland Security and maintains an element of independence from Counter Terrorism. Initially amongst these cohorts there was an emphasis on recruitment of scholars to provide a theological counter narrative or former extremists that can provide a sympathetic counter narrative. But extremism has evolved, and Channel panels can now find themselves supporting those that are referred to having a mixed or unstable ideology. This

in turn has placed Homeland Security with a conundrum and a likely rethink the knowledge and expertise of their providers. For example, a provider whose knowledge and/or experience of the right-wing extremism in the 1980's and 1990's may find themselves not understanding the radicalisation process in 2010's and 2020's. This is high likely to be as a result the introduction of cyber and emergence social media.

Chapter 3 - Understanding the the Risk from Cyber Extremism

This chapter documents an empirical study that was conducted in the Humberside Policing area with the intention of better understanding the risk to 16- to 18-year-olds from cyber extremism. There appears to be very little data that directly corresponds with a group that fit the current age demographic of PREVENT referrals in the geographical area under study. Furthermore, with the rapid change in both internet and the social media platforms enabled by them, Counter Terrorism policing and its partners may find itself in a position of not truly understanding what the current threat picture from cyber extremism is and therefore base its strategies and mitigating tactics on a purely hypothetical basis. The chapter is split into five sections; a literature review of cyber extremism, a detailed description of the methodology and the journey of gaining ethical approval, the findings of the study and analysis of those findings coupled with the authors experience as a pracademic in Counter Terrorism.

3.1 Literature review

Modern Counter Terrorism identifies and accepts that the risks from both terrorism and extremism have been largely driven by the digital revolution evolving into Web 2.0 (O'Reilley, 2009) and the mass usage of connected devices, specifically smart mobile devices. Not only has Web 2.0 given opportunities to change how terrorist and extremist operate online but give rise to new ideological threats that not strictly terrorist organisations but draw inspiration from established terrorist ideologies by advocating and encouraging the mass murder of sections of the society.

Cyber extremism is not a new concept, but it wasn't used that effectively until Islamic State was able to gain a foothold in Syria and Iraq and establish itself (Farwell, 2014). It was from this established footing that it was able to inspire and lure the influx of western citizens traveling to join them that they started to create an effective cyber based strategy (Awan, 2017). ISIS paved the way and unofficially created a model of how to be an effective extremist online where the adoption of social media platforms connected mobile telephone applications being the principal method of delivery. Their reach and online presence were hugely successful, and fluidity gave them the edge when embracing new emerging online cultures and trends with the aim of appealing to a much younger audience. The most reported example being the three Bethnal Green girls (Sage, 2015) whose journey to Syria and pledging allegiance to ISIS was heavily reported in the media, Shamima Begum being the most well-known of the three, and the negative effects of her actions still resonating today (Nyamutata, 2020). During the later days of Islamic State, they changed their online strategy from one looking to gain legitimacy by numbers to inspiring attacks from within the countries actively fighting or supporting efforts against them. In the UK this manifested into a variety of attacks but principally

involved what has become to be known as low complex attacks normally with an edge weapon. Whereas there are examples of working in conjunction with others, there is a real concern that an individual will take up their cause by becoming radicalised by extremist propaganda specifically designed to exploit a person's vulnerabilities whether they are sociological or misrepresenting aspects of the Islamic faith. The absence of a physical radicaliser and the opportunity to identify and intercept these third parties placed a real challenge to Counter Terrorism and their partners.

Even though Islamic State appears to have driven the trend of cyber extremism other extremist groups have embraced and noted the effectiveness and the reduced chance of detection and disruption. This has caused a perfect storm as far as using the internet to promote extremist thinking and hate, this is irrespective of the extremist ideology.

The next interaction and technological advancement being the ability and apparent popularity amongst this new breed of extremists to stream live images of terrorist activity, including beheadings, videos of bombs exploding and in relation to white supremacists the murder of New Zealand Muslims at a Mosque in Christchurch (Besley & Peters, 2020). The videos of which are still easily found on the internet today thus potentially inspiring others. The latter lone actor terrorist or as defined by UK counter terroism as self-initiated terrorists are the likely threat to the UK currently. The majority of the most recent attacks have been commited by indivduals whose antecedants would suggest they have never received any formal training or traveled abroad. Furthermore their radicalisation was done principly online. Lone actors traits have been subject to much research across all the extremist thematics (Katon, et al., 2021) (Bouhana, et al., 2018) (Hoffman, et al., 2020) (Gill & Corner, 2016) (Corner & Gill, 2015) (Clemmow, et al., 2020) (Ellis, et al., 2016) and all share common traits that can be manipulated or inspired by material seen online or more worringly the reaffirmtion of threat related grievances and necessity to use violence as a result.

Cyber extremism has been identified as being the predominant enabler for distribution and exposure to extremist ideologies and is highly likely to be the principal radicalising influence in the Humberside policing area (Counter Terrorism Policing North East, 2020). Counter Terrorism Policing and its partners are sighted on several differing methodologies and strategies that are available to extremist/terrorists at a macro level to further their aims and radicalise those that are vulnerable. However, there has been little empirical research looking at the risk from a micro level to ascertain what the threat picture looks like in a specific area of the UK and how and what material young people in that area are exposed to. There is a plethora of academic material (Costello, et al., 2016) (Chen, et al., 2008) (Hawdon, et al., 2019) covering the likely methodologies and effects of cyber extremism; however, this has mainly been qualitative and covers the internet as a whole rather than looking at its

effects on a micro level. In theory the threat and risks from cyber extremism should be universal with the principle enabling factor being access to the internet. Counter Terrorism policing produces documents covering local threats referred to as Counter Terrorism Local Profiles (HM Governemnt, 2012) and the purpose of these documents is to highlight the identified threat in these respective areas. The Counter Terrorism Local Profile for the Humberside policing area, which consists of Kingston upon Hull, the East Riding of Yorkshire, North Lincolnshire and North East Lincolnshire has consistently highlighted that cyber extremism is likely to be the principle enabler or source of inspiration for extremism and terrorist related activity in this geographical area. (Counter Terrorism Policing North East, 2020). This policing area has not been subject to a terrorist incident or had a high-profile arrest of a terrorist or extremist it can therefore be assumed with a degree of confidence that the possible effects from an individual extremists or group operating in a face-to-face capacity disseminating material and influencing or radicalising those in the wider community will be low. Meaning that any instances of radicalisation in this are highly likely to be from a cyber source.

The study's aim was to narrow the gap in knowledge on the risks associated to cyber extremism in the Humberside policing area while exploring potential criminological theories that may give insight into how and why young people may be attracted to or identify with extremist material online. It is the authors view that the study was successful in achieving its first aim but the study on its own did not give opportunity to determine a criminological hypothesis as to how and why people become radicalised by material associated to cyber extremism.

The study came from an assumption that the participants demographic is likely to use a mobile telephone or similar mobile device to access the internet rather than a desktop computer. This would mean that most of their access to social media platforms would be via applications that have to be downloaded from a virtual app store like Apple's app store or Google play. These applications are required to undergo a level of scrutiny and approval from the custodians of these virtual application stores and arguably places a safeguarding duty on them. This is also true to the application developers who too are likely to have their own terms of usage. The section of this chapter will detail the methodology of the study and the challenges and layers of ethical approval.

3.2   Methodology and Ethical considerations

The study was conducted during the middle of the UK wide national lockdown because of the COVID-19 pandemic when education provisions had reopened in a restrictive manner. This called for flexibility and agility and has likely prevented the full effective promotion of the study to the potential participants. All interactions with Multi-Agency Partnership board partners were done in a virtual manner and for several reasons it proved impossible to correspond with partners all at the same time.

Unfortunately, there was an element of inconsistency with the promotion of the study, its aims and the benefits to the colleges involved.

The Humberside policing area consists of four local authority areas, Kingston upon Hull, East Riding of Yorkshire, North Lincolnshire and North East Lincolnshire. All four local authority areas lead and administer their own respective Multi-Agency Partnership Boards (detailed in Chapter One) and it was through these boards that an agreement to commission this study in conjunction with the authors academic studies at the University of Hull. After deliberation with the panel, it was agreed that attempting to engage all students in further education in the Humberside policing area to complete the survey would be potentially problematic and it run the risk of becoming unwieldy considering the amount of volume that such an ambitious target would cause. Therefore, it was advised that the study should be a pilot for a potential larger study in the future. Furthermore, not all the further education providers in the Humberside Policing area are directly represented at the MAP board with many of the smaller providers relying on a single member to represent them all; however, the larger further education providers have the resources to have a dedicated 'Designated Safeguarding Lead' (DSL) and ten of these DSL's do attend across the four Multi-Agency Partnership boards. It was these ten colleges that were selected as it was felt that they would have the time and the resilience to realise their part in the success of the study.

The study centred around a survey targeting students aged between 16 and 18 years old. This demographic was selected firstly as they are legally children and therefore automatically considered vulnerable and subsequently places a legal duty on the Multi-Agency Partnership board to safeguard them. Furthermore, consideration was given to the participants maturity, given the nature of the topic under study, and their ability to complete the survey on their own. It was felt that approaching students younger than 16 years of age would be in appropriate and potentially invite criticism of the study considering the topic being covered in the survey. The fact the target audience is under the legal age to give consent it presented the study with an obvious ethics issue around gaining consent to participate, this is discussed in more detail later in this chapter.

The design of the study fostered and centred its ethics on four principles that under no circumstances could be breached, namely all the participants should remain anonymous indefinitely, the data obtained should not be used for advancement of a criminal investigation, consent must be obtained from all interested parties and lastly the data should be compliant with all current legislation around the sharing and retention of data in accordance with UK law.

To adhere to the first principle the study was conducted using a cyber enabled platform that could be accessed on either a desktop or a mobile device so to give the participants the choice of completing the survey at college or at home. This was imperative due to the high potential of disruption of COVID-19. This however brought with it some complexities around which platform to use and whether the platform adhered to data protection and the relatively new legislation associated with GDPR. Furthermore, the colleges couldn't agree on a single platform. Consideration was given to using a platform commissioned by the University of Hull, who were the supervising institution of the author, but was rejected due to further complexities around the storage and retention of the data harvested. The design of the study aimed to keep the colleges empowered and remain the custodians of the data associated to their learners. This in turn gave them the option of withdrawing from the study right up until they shared the data with the relevant MAP boards via Counter Terrorism policing whose role was to conduct the analysis. To overcome the issue around which platform should be used the problem was looked at in reverse. To complete the analysis, it was preferred for the data to be presented in a Microsoft Excel spreadsheet. Guidance was then given so that any platform that adhered to all the study's principles and had a feature that allowed the data to populate an Excel spreadsheet can be used, but a further condition was made that the platform used must have a facility to have a landing page before commencement of the survey. This landing page was used to communicate with the participant and explain to them what the survey was for and allow them the option of choosing to complete the survey (principle three). Most of the colleges selected the Microsoft forms platform as it became a no cost option for them, but survey monkey was used by at least one college.

Even though both Counter Terrorism policing and Humberside police have had sight of the data there has been no attempt to use the data in any other manner than in the spirit and purpose of the study.

The gaining of ethics approval from the University of Hull ethics panel and consent from all the parties was especially problematic. The universities ethics panel were a little nervous when endorsing the study. Firstly, the universities guidance is that master's students, which the author was, should not normally conduct a study with those under eighteen; however, there was acknowledgement that the author being a serving police officer in Counter Terrorism was unique amongst their academic peers due to the fact it was normal in their professional role to have access to and worked alongside professionals charged with the safeguarding of children. This became a double-edged sword as it added a layer of complexity which demanded careful consideration and disclosure as to when the author was acting in their professional capacity or as a master's student with the university. This was

especially true to maintain the integrity by being transparent with the participants and the parent/guardians when gaining explicit consent.

The individual colleges were asked to utilise there already established relationships and communication gateways with their learners' parents/guardians and to promote and explain the purpose of the study and to gain their consent for their children to participate. The author devised a form of words which explicitly explained the four principles to give reassurance and allowed questions or enquiries to be asked. The positive consent responses were collated by the colleges who then sent the link to the relevant children. A consequence to this method is that it introduced two 'gatekeepers', namely the parent/guardian and the participant themselves. Furthermore, if the college felt later that they couldn't commit or the results may reflect badly on them and their professional reputation, they too could choose whether to participate or not to disseminate the results. All three negative outcomes feature during the period of study and are discussed in the analysis and reflection sub-categories of this chapter.

The university ethics panel further sort assurances on the handling and storage of the data obtained again due to the uniqueness of the study, by the fact it was being done in partnership with several authorised bodies. The study's design meant that the individual colleges were the facilitators of the survey and remained the custodians of the data rather than one body like the university themselves. It was noted that the colleges were already experienced in handling sensitive data and had the capability of storing the data in line with current legislation so there was no need to create something new. The study also took advantage of an established 'Information Sharing Agreement' (ISA) between all the MAP board partners, which includes the colleges, borne from a necessity to understand what local Counter Terrorism threats are likely to be in a geographical area. This shared data from partners is assessed alongside other forms of information that is then detailed in the CTLP (Chapter one). Therefore, the study other than adding to academic knowledge had a collateral benefit of enriching the CTLP and national threat picture concerning cyber extremism.

The survey itself consisted of a landing page which detailed the purpose of the survey and the four principles. This was then followed by nine broad questions that contained differing number of sub-questions depending on the participants answer to the broad question. The questions were a mixture of open and closed questions. The open questions to seek statistical information and the open questions to seek context. The questions and the question workflows were constructed by the author but each of the respective colleges programmed them on their selected survey platform. The survey ran for a period of two weeks immediately after the learners returned from the Easter break.

3.3 The study's findings

Across the Humberside policing area 1441 students completed the survey. 52% were from the East Riding of Yorkshire, 23% were from North Lincolnshire, 20% from North East Lincolnshire and only 5% from Kingston upon Hull. The latter being the most densely populated area with the geographical study area and therefore it was hoped that Kingston upon Hull would have been the biggest contributor.

The study initially looked to understand what platform were being used to gain a better understanding as to whether extremist material is shown predominately on fringe platforms and areas of the internet or whether such material can be found on the more mainstream platforms/areas. The participants were asked to select the most three used mobile telephone applications from a list of eleven and given the opportunity to select other. The apps offered were snapchat, Instagram, Facebook Messenger, TikTok, WhatsApp, Discord, Twitter, Telegram, GAB, Tumblr, and YouTube. From the 1441 participants 2308 apps were selected and broken down as follows

SnapChat	Instagram	Facebook Messenger	TiKTok	WhatsApp	Discord	Twitter	Telegram	GAB	Tumblr	YouTube	Other
533	441	391	272	238	217	122	10	4	2	2	76

The participants were also asked about if they consider privacy, end to end encryption or time delete as an important functionality when selecting which mobile telephone applications to use. 64% said they didn't and of the 36% who did the vast majority cited the need to protect themselves and their family from online hackers rather than trying to hide what they were doing with a common comment made by the participants being along the lines "I have nothing to hide". There was a very small number who did make mention of preventing the "government from spying" on them and "blocking the CIA" though.

The next phase of questions explored whether the participants had been exposed to online racist or religious hate speech that was also promoting violence towards others. Results of which showed that 32% of the participants had and, with 73% of this group highlighting that said material came from an anonymous source. The results were further broken down into thematical areas with the results showing the following legally protected characteristics being the target of the hate.

55% towards black ethnicity

19% towards the LGBTQ+ community

16% towards the Muslim faith

6% towards Asian ethnicity

4% towards the Jewish faith

Those participants who had seen material associated to hate were asked to express how they personally felt after seeing the material. Encouragingly 63% of the participants felt angry about its existence. 15% felt intimidated, 12% felt the material was humorous, and the remaining 10% was split evenly between those finding the material interesting or supporting the messaging contained within it.

The study moved on to establish whether any participant had been directly messaged by any group or individual who the participant felt was an extremist. Overwhelmingly 97% of the participants said they hadn't. Of the 3% who had the extremist thematical areas were broken down as follows: -

21% from religious extremists

11% from right wing extremists

9% from left wing extremists

5% from those not considered to be affiliated to a thematical area

54% where other was selected

As well as encouraging the participants to select a thematical area they were asked if they knew the name of the extremist group associated to the person who had contacted them. The groups identified were Antifa (Antifascist), BLM (Black Lives Matter), National front (Right wing), Neo-Nazi (Right wing), an unnamed Christian group and a Vegan group.

The third question area sort to understand whether the participants had either deliberately or inadvertently watched a video associated to extremism where images of violence was depicted. Of note there was over a 50% drop in participants answering this question compared to the previous two. Of those that did participate 15% had seen such images and were encouraged to explain what they saw and on which platform. Of those that responded to this element of the question the answers were.

- *I saw a beheading on TikTok*
- *I saw on TikTok someone cutting someone's head off I think it was ISIS*
- *ISIS*

- *reddit/ best gore.com*
- *Videos of a mosque getting shot up, posted online*
- *Just online, go to reddit, live leak etc. and the things you find there is worse than the dark web*
- *Lots of messed up stuff on discord and reddit and when KIK existed it was always being shared and you can still find websites like 'running the gauntlet' which show gore and terrorist beheadings and stuff there's also a website you find it all on that begins with v something*
- *Violent videos including ISIS beheadings and genocide on a facebook messenger group chat which was made to share gore content*

The fourth question area explored the participants use of message board forums with the only example being reddit and whether in the participants opinion these platforms have become more extreme or contain more extremist content. On reflection this question area needed to be separated into two distinct questions to get a better understanding when considering the results obtained. Besides this only 9% of the participants said they used message boards and considered that they contained extremist content. As well as the study introduced forum reddit both 4Chan and 8Chan was mentioned by some of the participants. Like before those participants that had seen perceived extremist material were asked how they felt about the material and encouraged to comment.

- *I don't like it but it's entertaining to read*
- *I mean, people with always have extremists' views and you can make as many sub reddits as you want that idolise your views, you can't stop it, you can just limit the attention it gets before being shut down*
- *It's become more of a joke rather than a serious issue over the past few years. People joke about extremism but now it's hard to tell where the line is drawn between joke and seriousness*
- *Literally any internet forum, there is worse stuff on popular apps like twitter, facebook etc. than "underground" forums, this is not speaking from personal experience but rather I am quoting a social media influencer and tech expert who I whole heartedly agree with*
- *I feel that because people are more accepting of other people and at first that was fine but then a lot of people on the internet take too far and instead of just being happy that people are accepting a particular group, they bring down others that are not part of them and in turn they retaliate, and it just ends up going in circle and make the situation worse instead of making it better*
- *During the years of western involvement in the middle east more and more people have become racially aggravated towards these groups*
- *People think it's funny dark humour*
- *I personally have not taken into consideration if there is an increase in extremist content, my brain typically just filters the content out automatically and continues to look for content which I actually want to see*
- *I don't follow any extremist or weird sites like that its mainly just memes and shit*
- *On Twitter I was viewing a very positive post by Essex Police promoting diversity within the force and within the comments section of said post I saw an account making hateful remarks in regard to the post and within their profile picture was a logo linked to the British Union of Fascists. The fact that someone could even be on any social platform with a Profile promoting the British Union of Fascist is awful especially with the hate and division they cause*
- *Don't see any, but if I did, I wouldn't say anything in case of threats*

In addition, the participants also shared comments surrounding themes and the identified messaging boards used by them.

Reddit

- *No change. reddit can be a safe place for extremists*
- *I use Reddit to read about shows that I like but trolls sometimes try to ruin by posting extreme stuff*
- *Reddit is especially disgusting with all of the KKK and Nazi content, so I stopped using it within a month due to the fear and anger. There is also a side of TikTok that is filled with pure homophobia and hatred which scares me too as these ideologies are starting to impact 12-16 year olds and hate crimes are more common. I also believe that promoting rape, sexual assault and sexual abuse is promoted due to the lack of consequence and/or people believing survivors.*
- *Reddit used to be known as one of the most toxic places on the internet and now is one of the most supportive, welcoming, and kind places on the internet. I myself haven't seen any extremist related activity on reddit.*
- *Reddit has become quite anti-Semitic.*

4Chan and 8Chan

- *Racism and extremism are bad :) just check /Pol/ on 4chan and basically all of 8chan*
- *4chan is just extreme by nature so it's not surprising to see extreme left/right wing viewpoints there.*

General comments

- *I think the increase in extremism has become commonplace online because of pushback against groups like BLM*
- *The BLM movement set off a lot of racism, the recent women's movement set off a load of creepy incels who think it's their right to abuse women and they've been trying to track down girls who speak out about rape, etc and are making threats that I've seen, COVID has sparked a lot of Asian hate and hate against young people even though the old people are the ones not wearing masks.*
- *After the Sarah Everard Vigil, The BLM Protests and Covid-19 I've noticed a significant increase in posts with generally angry or malicious-sounding content, probably due to the large amount of controversy surrounding The Vigil and BLM and Lockdown causing more extreme people to spend more time online as a result of isolation as opposed to normal*
- *The right feel as though they're being oppressed and silenced because someone somewhere is saying something different from them, so they act out with violence, as per usual. These kinds of views are scattershot throughout the internet with no particular board (to my knowledge) other than the previously mentioned facebook and 4chan (the latter being more prominent in its hosting of right wing users), then there's also the various misogynistic incel forums and the like on reddit, not to mention Men Going Their Own Way (or MGTOW) who take pride in their*

active misogyny and pinning all their misfortune and gripes with society on women as opposed to the incels who simply lament about not being given their "rightfully deserved" girlfriend (and also sex).

The final series of questions sort to understand how confident the participants were in reporting, if they chose to do so, the presence of extremist material on the internet. Considering that some of the participants recorded that they had not seen or been exposed to extremist material it is accepted that this question would be purely theoretical for some, but still holds validity as far as gaining an understanding on the likely intentions of the participants. 84% of the participants when asked said they knew how to report concerning material found on the internet. Follow up questions sort to clarify who or which professional body they would report it to. A quarter of participants stated that they would just ignore the material and therefore the matter would go unreported. A further quarter of the participants stated that they would bring the matter to their family's attention. The remaining half of the participants stated that they would report it to the police (24%), to their friends (14%) and lastly to a member of staff at the college (12%). This question also teased out a participant linking Incels with extremism. The current view of Counter Terrorism is that Inceldom is not an extremist ideology; however Counter Terrorism officer involved with Incel's. This is covered more deeply in Chapter 4.

The participants were also asked on a scale of 1 to 10 how much they felt at risk from cyber extremism the average score was 5.5. Those participants that scored the risk as either a 9 or 10, 37% had seen extremist or hate material, 19% had watched videos considered extreme and 15% of this group used messaging boards. Compared to those who scored a 1 or 2 only 16% had seen extremist or hate material, just 4% had viewed extremist content and 8% used messaging boards. The last aspect of the study asked whether the participants had heard of the Counter Terrorism PREVENT strategy which showed 54% hadn't.

3.4   Analysis and Discussion

It is accepted that when labelling and determining what is and isn't extremist material becomes subjective depending on who is viewing the material. Whereas the UK government has published a definition (Chapter 2) it is likely that this has not been seen by the everyday public and therefore does not constitute as an effective guide to large parts of society; however, society has been exposed more and more to extremism and terrorist related activity through mainstream media reporting, so there can be a degree of confidence that by in large society has a good idea what content should be considered as extremist material.

Returning to the previous questions highlighted at the start of this chapter namely, what are the current trends, what extremist and hate material have the participants seen and how confident are the participants in reporting concerning material? The study indicates that extremist material is easily found and shared on mainstream social media platforms. Whereas not part of the study there is still a likely misconception that extremist material is confined to fringe platforms, like GAB, with calls to suppress or remove such content (Van der Vegt, et al., 2019). This is particularly hard as the internet is global and subject to differing standards and laws across the globe with no universal definition or consensus on the matter (chapter two). The fact the study has shown that extremist material is available on mainstream platforms would therefore call for a rethink as to how society safeguards vulnerable people online. There are recorded attempts by mainstream social media platforms attempting to seek out and remove content with the aim of reducing the amount of negative material on their platforms but what is clear is that the likely volume of such material is overwhelming and the governance and enforcement of the platform's terms of use. Resulting in an inference that there is an unwillingness to allocate more resources to tackling the problem or develop an effective technological answer to remove such material in an automated manner due to the cost it would likely incur. Therefore, education and awareness must be the most effective tool to mitigating harm. But this comes with its own problems. Technology and how it is used has exploded causing a mismatch in awareness between young users and many parents, teachers, and safeguarding professionals. The author has witnessed this first-hand when working with children's social care whose strategies and procedures are along the lines of removing the negative influence from the family home, normally a physical person. But when the negative influence is directly enabled by access to the internet applying such a strategy by looking to remove a child's access is not a reasonable response considering the potential harm of isolating the child from their peers and the opportunity for them to communicate in the manner that they do. Furthermore, isolating a person from positive peers and the wider society is seen as one of the fundamental causes of someone becoming vulnerable (HM Government, 2020). This can be frustrating and ultimately leave the safeguarding professional with very few options which will not affect gaining true co-operation from the vulnerable person and those around them. The author has also witnessed an unease from other agency professionals who are not experienced with safeguarding those from radicalisation to even speak with a vulnerable person about the matter and fail to see the similarities associated with radicalisation compared with other forms of exploitation. This can cause conflict with an insistence that a counter terrorism officer must be present even though this may appear disproportionate in the circumstance. If those safeguarding professionals whose role is not fulltime in counter terrorism it is likely that they may have knowledge gap, and this is reflected to a in a greater degree with the wider public who are also unaware of how someone becomes

radicalised. Attempts to mitigate this by the promotion and distribution of awareness campaigns concentrate on a faceless third party who gains an element of control over a loved one and encouraging them to commit an act. Whereas the study has shown is these publicised examples are highly likely to be a rarity and it is more than likely that vulnerable people will become inspired by extremist material on the internet and radicalised in an indirect manner. This has sometimes been labelled as self-radicalising, a term that is misleading and counterproductive. This is addressed later in this chapter.

The study also shows that well publicised media events can have a bearing on what extremist/hate material starts to be circulated. The study was conducted immediately after the Easter break (April 2021) which was around a month after the Megan and Harry Windsor interview with Oprah Winfrey. The interview amongst the many themes discussed included racism. Furthermore, the Black Lives Matter (BLM) movement before this was very much in the news and there were several incidents both in America and the UK where the group was challenging the structuralism of both countries concerning racial equality in society. The inference from the study's results is hate material seen was pushing back against BLM and the Oprah interview resulting in material directing hatred towards the black community. What was absent from the list was hate material directed towards feminism. It is probable that if the survey was conducted during the height of the media reporting into the manner of how Sarah Everard was murdered and the calls from some for all men to take responsibility for her death, feminism, and the rejection by some would have been the catalyst for the sharing of hatred material towards women. The consequence, if this inference is accepted, is that the study has a very short shelf life as far as understanding what thematical area is likely to be the target of hate for a sustained period and therefore the author would not be recommended to use the findings to support a long-term strategy to intensify resources for the protection of a single protected characteristic over others, even in the face of political pressures.

The study has shown that it is very unlikely for a person to be contacted by an extremist directly. This is likely due to the risk of the extremist's identity being compromised. The internet to a certain degree provides a level of anonymity and potential safeguards for the avoidance of law enforcement. This anonymity can also be true to the identity of the person the extremist is talking to adding another layer of complexity for safeguarding professionals to identify and safeguard vulnerable people purely in cyber space. The consequence being that there may be many people being subjected to negative material who will never come to the attention of the safeguarding professionals. The author has observed individuals and groups associated with extremism using 'vetting methodologies' to firstly make sure that the person they are corresponding with is not a member of law enforcement and

secondly they are not a counter movement or journalist looking to expose them. Meaning it is more likely that the online radicaliser is watching for comments or 'tells' that would indicate that some is vulnerable before approaching them or encouraging them to join an online forum whose membership is carefully monitored, and their anonymous identity is maintained. The study has shown that 10% of the participants found the hate material they saw as either interesting or supported the comments or theme of the hatred. If any of the 10% openly commented on or shared the material they could be inadvertently advertising (Scanlon & Gerber, 2014) that they are vulnerable and depending on the platform's functionality, like private messaging, and the source who shared the material may be advertising their vulnerability or put them in the spotlight for more material to be directed towards them hoping the vulnerable person creates an echo chamber of hate (Bright, 2017) (Hollewell & Longpré, 2021).

Building on this the study does provide comfort by highlighting that it is highly unlikely that a vulnerable person will see material directly associated to extremist ideologies; however, most of the material described in the study was videos of beheadings. What the study was not able to do was understand whether the material was being shared to radicalise or whether there was an element of morbid curiosity on behalf of the publisher or the viewer. What can't be disputed is that depending on the viewer and how often they have been exposed to such material there is a potential increase in risk in a vulnerable person becoming radicalised and normalise violence or being in the presence of such violence. An arguably critical element to increasing a person's capability to commit a violent extremist act. Whereas the beheadings were largely attributed to religious extremism with the Islamic State being specifically named by the participants. One participant described what is likely to be the recording of the Christchurch Mosque shootings which was committed by a white nationalist. Again, the video by design or otherwise has been shared multiple times and it could be expected that a minority of viewers will be either inspired or desensitise themselves to the fact that lives where were being taken especially as you could draw similarities to how the video was recorded and presented and the images gamers see in modern first-person shooter game by looking at parallels from the concerns over the militarisation of young players by first person shooter games (Hitchens, et al., 2013). When highlighting an increase in capability, a misconception would be to only consider the access to materials or funds that enable a person to commit or support an act. But in respect of committing a violent extremist act a potentially overlooked important aspect is the mental readiness to commit multiple murders. This is especially true in 'low sophisticated' attacks by self-initiated terrorists formerly referred to as lone actors. These 'low sophisticated' attacks in the UK are highly likely to involve an edged weapon, due to the ease of obtaining one compared to an explosive device or firearm, and therefore exposes the attacker to the raw emotion and pain of their victims. This proximity and

the closeness to the victim demands for the desensitisation (Vale, 2018) and the normalisation of being around such emotions to become an effective multiple killer which makes the videos and images described in the study an essential tool for radicalisers and are not chosen just to glorify their cause. Earlier the subject of self-radicalising was introduced. The misguided notion of self-radicalising being that a person chooses to be an extremist and actively seeks out associated material to reaffirm an ideology they already have (Hollewell & Longpré, 2021). This misconception could fuel or give a mandate that those that are undergoing or have been radicalised are future offenders that need to be stopped and should be subject to enforcement or disruption and the hands of the police or similar. This study contradicts this theory by highlighting that extremist and hate material can quite easily be viewed inadvertently and depending on sociological issues past or present, including the structuralist environment surrounding them (Schmid, 2013). Therefore, the study supports a strong argument that those that are being radicalised or have been radicalised, having not committed a criminal offence which terrorism is considered, are instead the victims of radicalisation and first consideration should always be to support and provide treatment or intervention to counter the negative ideology they have been exposed to without any form of negative judgement on the part of society. This non-judgement is imperative if the PREVENT strategy is to be successful as the study indicates that most instances that would be considered a PREVENT matter are not going to be referred. The author having sight of all PREVENT referrals in the geographical area under study can comment that a very small number of referrals are received from family members or from peers in a vulnerable person's age group directly. This would then raise the potential for missed opportunities to potentially 89% from the study's recorded 25%. This unacceptably high percentage would necessitate a rethink on how PREVENT is delivered and promoted especially to friends and family. This is especially true concerning adults who are likely to not be in contact with professionals who are likely to have deontological mindset to the circumstance considering the PREVENT duty.

On reflection if the study is to be repeated there needs to be some modification to some of the questions sets. Some of the questions allowed the participant to choose 'other' without a further part question allowing them to populate their answer in free text. Consequently, this means there has been a missed opportunity to identify other possible apps that are being regularly used. Interestingly the study listed all the extremist thematical areas used by Counter Terrorism but 54% of the participants who answered the question surrounding which extremist area associated to the extremist who contacted them directly other was also selected. This may show that there is lack of understanding on how extremist groups are defined or their view of extremism is different. Whereas it is only speculation if the subjects were referring to Incel's they are a good example of a sub-culture that has been misunderstood as an extremist ideology. Incel's did feature in the study and were referred to as

extremist but current thinking by UK Counter Terrorism is not to consider Inceldom as extremist ideology. The next chapter looks at Inceldom and considers whether it is or is not an ideology and details the current police response.

Chapter 4 – Incel, An Extremist Ideology or Violent Sub-Culture?

This chapter was never planned but has become pertinent not only by the study but by an event that has occurred in the UK where Jake Davison who announced his identification with Inceldom committed multiple murders with a legally owned firearm. The first part will explore the emerging sub-culture of Incels, and their belief system. The second part will detail how Counter Terrorism mitigates a potential threat from Incels and submits an answer as to whether Inceldom should be considered an ideology and their actions a form of misogynistic terrorism.

4.1 Inceldom, a whistle stop tour

Some of the participants in the study highlighted and associated the Incel-subculture to extremism. This is timely after a recent event in the UK brought Incel's to the attention to most of the British public. Jake Davison identified with the Incel sub-culture and expressed so in YouTube videos. He later went on to kill his mother and four other random members of the public, one of which was a three-year-old girl. Initial media reporting, heavily associating the deaths with his identification with Inceldom. There were calls from some that the murders should be considered a terrorist act and recognition that Inceldom was an ideology; however, UK Counter Terrorism has resisted these calls and still does not consider Incels as extremist or their actions as a form of misogynistic terrorism. Furthermore, this is the first homicide in the UK that has any known links to Inceldom so it is hard to argue that officers in the PURSUE thematic of Counter Terrorism Policing should be actively investigating those that may have links to Inceldom over those individuals and groups that have an established history of committing violent extremist acts or terrorist related offences.

Unlike other threats you would expect the UK Counter Terrorism Policing to be targeting the Incel movement is not a structured organisation or group with a clear structure Van der Veer (2020). There is no membership nor herical leadership dictating the direction of the sub-culture. Instead they are a collective brought together by a misguided bond. Inceldom's roots are with a gender-neutral online support group created by a Canadian female who was struggling whilst she was studying at university to form romantic and sexual relationships. However, her concept was hijacked of sorts and the idea of Inceldom underwent several iterations migrating away from the original support page and finding a home on online messaging board sites 4Chan and Reddit where it distanced itself from its roots and the rhetoric became more masculine orientated (Hoffman, et al., 2020). These messaging boards enabled the culture to evolve into what some has be described as the 'Manosphere' with Incels being the most outwardly extreme with some Incel's advocating violence. Papadamou, et al (2020)

highlights that the 'Manosphere' is split in to four broad categories. All four identify with a rhetoric that has an anti-feminist sentiment while others associate the movement with male supremacy (Van der Veer, 2020) (Van Valkenburgh, 2021); however, it was the Incel's who displayed the advocation of violence towards women (Hoffman, et al., 2020). This stemmed from a fundamentally misguided hatred towards women from the belief that the Incel due to their physical characteristics are not attractive to females (Maxwell, et al., 2020). Furthermore, Incel's subscribe to the belief that all females are shallow and are only attracted to males on the visual plane and do not value intellect or personality. The culture has created its own stereotypical caricature with attractive females taking on the guise of a female with long blonde flowing hair, large breasts, wearing short dresses and high heels and referred to as Stacey's. The male equivalent, Chad's, having the chiselled face and athletic physique you might expect from a top-level sportsman. The lessor of these categories includes the female Becky's and the male normies. The Becky's are normally depicted as being brunette dressing conservatively and educated, but like the Stacey's yearn for a sexual relationship with a Chad but settle for relationships with Normies (Menzie, 2020). This leaves the Incels the lowest of the categories with no hope or chance to have a sexual relationship.

This then gave rise to an Incel sub-belief system referred to as 'black pilling' (Cottee, 2021) (Regehr, 2020). The term and meaning of taking a pill came from the movie 'The Matrix where the main character in the film was living in a simulation where he is offered two pills of differing colours by another character but is given a warning before the choice is made. The blue pill if swallowed returns the person back to the simulation with all memory of the pills and the choice they made erased meaning that they can live out their life in enslaved ignorance with their future determined by a faceless third party. The red pill denotes awakening and releases the person from mental emancipation, but into a world that is harsh and full of challenges but grants you free will to choose your fate. The scene is heavily used in many conspiratorial beliefs borne from the meme culture of 4Chan (O'Malley, et al., 2020) (Ging, 2019) (Van Valkenburgh, 2021); but some in the Incel subculture have created the 'blackpill' which has a lot of similarities as taking the red pill but the free will you have obtained is futile as every choice you make will always come to a negative outcome and there is nothing that they can do about it. This feeling of hopelessness and the eventual transition towards hatred mirrors Robert Agnew's first major strain in his General Strain Theory (Agnew, 2010) (Brezina, 2017). This anomie and the Incel perceived de-masculinisation reinforce the digital hegemony created by them Ging (2019) and there are examples that on rare occaisions they have transcended into real world with devastiing consequecnes. The American Elliot Rodger is probably the most infamous of all the Incel's who progressed to murder.

Elliot displayed many traits and the manner in which he commited his murders does allow comparisons to be made to those labelled self intiiatated terrorist (Hoffman, et al., 2020) (Bouhana, et al., 2018). In 2014 Elliot Rodger released his manifesto as to why he felt he was marginalised based on his perceived injustices caused by his own intersectionality, namely race, class and gender. The latter heavily associated to his misconception of what it was to be masculine and blaming a perceived biological inadequacy on why he was not attractive and rejected by women. It could be argued then that Rodger subscribed to the 'black pill' belief and that is why after killing? people in the name of Inceldom, through his video manifesto, he turned his weapon on himself and took his own life confirming that he felt he had nothing to live for. Rodger became a role model in the Incel sub-culture with those that are flirting with or threatening to commit murder referring to doing so as 'doing an ER'. The next section of this chapter details the current UK police response and puts forward an argument from the authors point of view as to whether Inceldom is an ideology and appropriate and proportionate Counter Terrorism policing resources be diverted to mitigating an emerging threat.

4.2   Incel and UK policing

After the murders in Plymouth some media reporting and commentators where surprised or dismayed that the UK's Counter Terrorism policing did not lead the investigation to the circumstances leading up to the murders. In the aftermath the offender Jake Davidson was exposed as being an Incel and sections of his videos that he shared on YouTube were shared with the nation by the media. From some there was an immediate call for Incel's to be deemed as terrorists and their beliefs as an extremist ideology. This never happened as an assessment made that the murders were not terrorism related and the matter was to be investigated as multiple homicides. Counter Terrorism officers did provide expertise and resources to Devon and Cornwall Police's murder team. What was not highlighted was that Counter Terrorism officers in PREVENT were and had been involved with those that identified with the Incel sub-culture for some years. The author being one of those officers.

Chapter one described how Counter Terrorism policing is split into four thematical areas. The PREVENT thematic which largely operates where no crime has been committed and supports vulnerable people that are at risk to radicalisation. PREVENT had already started to provide support to those that identified with those that fantasised or had a desire to replicate an American school shooting like the tragic events at Columbine in 1999 but hasn't quite rightly designated it as an extremist ideology. Also, in chapter one the three broad assessment for areas for PREVENT relevancy namely, engagement, capability, and intent (HM Government, 2020) were detailed. Building on this desensitisation was introduced in chapter two. Desensitisation being detailed as an essential element to increase a person's capability to commit a violent extremist act and in the study conducted there was

documented instances of images depicting and glorying violence and suffering was being shared and received. This is also true when a person is exposed to an online echo chamber glorifying and encouraging the mass murder of others and consequentially having the potential to raise a person's capability and intent to a lesser degree to want to commit a violent act. It would therefore only require a would-be radicaliser to convince a person to change or divert their anger so that they started to engage with their ideology whilst maintaining their capability and intent to act for a violent extremist incident to occur. It's from this perspective that Incels should be considered along the same lines those identifying with school shooters.

PREVENT and policing generally finds itself with a real challenge deciphering and assessing which Incels identify with violence and those that either standby (lurking) or are 'keyboard warriors' on Incel related cyber platforms. It is arguable that if there is no likelihood of a criminal offence or a threat to the community then why should police officers time be consumed. It would be an inappropriate use of resources to treat all Incels the same. Therefore, PREVENT and general policing need to understand and prioritise resources based on perceived risk to determine which Incels they need to engage with. An option would be to consider whether they identify with the Matrix pill scenario or more poignantly if they believe their life has become 'black pilled'. The outcome, if acted upon, is likely to be the taking of their life, but can easily include the murder of others as well. In the aftermath of Davison's murders, the vetting of ownership of firearms was called into question with questions being asked as to why Davidson's social media accounts were not checked before allowing him to have a firearm. In response a proposal was put forward that all applicants should be asked about their social media accounts and then interrogate them afterwards. This is understandable in principle but ineffective in practice. This proposal would call for honesty on behalf of the applicant to disclose all social media accounts that they have as it is possible that the account may be created in synonym name or may have high privacy settings preventing the police from seeing the content. If this was suspected, then the police would have to attempt to use covert policing methods governed by the Regulation of the Investigatory Powers Act which may not cater for what could be considered a fishing exercise as opposed to a targeted criminal investigation. Notwithstanding that some might argue that this would be a breach of article 8 of a person's human rights and be disproportionate evasion of privacy. Furthermore, the tactic would be very short lived as those looking to apply for a firearm legally knowing they would be subject to a social media check would logically delete any accounts before doing so. The largest flaw with this is there is an uninformed belief that the that threat from an Incel related murder will be enabled by a firearm. This is not likely to be the case in the UK and parallels can be drawn from attacks by self-initiated terrorists which predominately utilise low complex attacks with an edged weapon.

The author would advocate being opened minded to a possibility that Inceldom will splinter and change. Currently the belief system is looked through a lens of biological essentialism with an emphasis on white, heterosexual males being the likely offender and heterosexual females the target of their hatred. But by returning to Incel's origins it is not beyond the realms of possibility that all forms intersectionality coupled with a belief of entitlement to sex with a partner of your choosing could be considered or lead to a person to identifying as an Incel.

Considering the questions as to whether Inceldom is an ideology, after its linkage by a research participant, there is one defining issue that doesn't make it an ideology. Without trying to ignore the complexities of associated extremist ideologies and putting coercion to one side. All ideologies allow the subject to choose whether they want to identify with the ideology; however, Inceldom comes from a perception that you do not have a choice. Their physical biology and the fact they feel they will never be attractive to a female is a consequence. Therefore, in theory no Incel wants to be an Incel but identify with the term to label themselves to share their perceived injustice with others.

Considering the involvement of PREVENT and Channel panel (Chapter 2) this concept of consequence calls into question the effectiveness of Home Office Intervention Providers. No longer are the providers being asked to draw someone back from an ideology but instead they are trying to instil a new belief system that attractiveness in the eyes of another is more than just physical, and in respect of those Incel's that identify with 'black pill' that their life does have hope and opportunity; however, this new challenge and approach should not be considered as evidence to withdraw PREVENT and the professionals that work in this thematic. PREVENT has developed and learnt to support and manage individuals that have not committed a criminal offence but have flirted with, or who have encouraged others to consider committing a violent act on a large scale out of hatred or because of a hatred of another. The author at the time of writing knows of no other agency or department that has the experience and expertise to carry out this specialist role and has governmental oversight that can be held to account for their actions.

Chapter 5 - Conclusions

The study has been successful in achieving what it set out to achieve both academically and strategically from the Multi-Agency Partnership board perspective. Concentrating on the academic merits associated to the study it provides evidence that there is validity in exploring cyber extremism on a geographical micro level to gain an understanding the threat, risk, and harm on a national macro level. Furthermore, the fact the internet is universal, small elements of the study can form as evidence at an international level. This requires caution as the further outward you expand the less pertinent the results due to other countries favouring or having access to different cyber platforms compared to most western countries. The study does have a short shelf life considering how quickly technology evolves and cyber trends change. That being the case the study needs to be expanded with consideration for comparisons to be made with other areas of the country. The author is already in the process of doing this with a London borough, the current likely comparison location.

To enhance concluding the studying the author will provide some further context from a Counter Terrorism practitioner and their experience of being directly involved in supporting and managing subjects identified as being vulnerable to radicalisation. Considering the results, the author has come to an untested hypothesis that identity is becoming the principal vulnerability to radicalisation from a cyber enabled or inspired radicalisation. Web 2.0 and the emergence of social networking platforms have given a rise for the opportunity or desire for some to reinvent themselves in the cyber space which is far more difficult to do in their real-world life or at the very least would take them significantly more time and energy to do so. This real-world life is a journey where a person's historical experiences, whether positive or negative, forms a wake in time as they progress of the life path with the experience of doing so resonating with them for all time. This hypothetical wake cannot be changed, altered, or largely forgotten; however, this is not true for the cyber world which gives a person the opportunity to choose, modify or completely change every aspect of their intersectionality with a key stroke. Meaning those that have undergone or undergoing strain in their life may look to the cyber world for escapism and depending on how in invested they become they may elect to reinvent themselves entirely and consequently start to resent their real-world persona and choosing to spend more and more time online. The author has observed vulnerable people even stupefying themselves with illicit drugs or alcohol to avoid having to live their real lives, with sobriety to a certain degree only occurring when they are online.

When looking more deeply at identity caution should be exercised purely considering it in a dualistic manner namely, the real world and cyber world. But instead to include an added layer of perceptions

when looking at identity. Social media and to a certain degree materialism can give rise to the altering a person's perception of what everyday life should look like and place a strain on them by making them believe they are failing (Brezina, 2017). The feeling of discontent fuelled by this false perception of normal may isolate and bring loneliness along with other vulnerabilities fed by this disconnection creating the perfect opportunity for an extremist to attempt to introduce an idea of injustice caused by whoever their ideology targets. Furthermore, when it comes to cyber if a person is creating a different cyber identity to their real-world identity, they will no doubt have an idea of a perception they wish people to see; however, this perception may not always be received in the manner intended by a third-party creating a different perception to the intended identity and whether the person is aware or not may cause strain again on them. Whereas these perceptions can occur at any time in person's the authors experience would support an inference that this is more likely to occur just prior or immediately after they enter adulthood whereas a consequence they are in period of transition and attempting to understand where, how or what expectation in the adult society. It is during this time that said group will have unrestricted and unsupervised access to the internet. Furthermore, they are less likely to be in receipt of professional support as many services drastically drop off when a person becomes an adult, sometimes referred to as aging out of the system.

The internet and the social media platforms enabled by it are overall a force for good. They allow people to connect and share ideas like ever before. But it can also make people feel very lonely by not allowing meaningful relationships to take place. Furthermore, the same sites being free and to obtain revenue streams from elsewhere and this is normally the selling of personal data or the targeting of advertising. Consequently, this fosters materialism and normalises the haves and the have nots increasing further anomie and the likely discontent that comes with. Anomie then becomes an enabling factor for why before someone who normally ignores online extremist material starts to consider the ideology because it promises a better life, like the Islamic State did when encouraging travel to Syria, or it gives a likely target to blame for a perceived injustice. These turns of events are still a rarity but the consequences when a vulnerable person is mobilised to commit a violent extremist act can be catastrophic, especially considering the threat from self-initiated terrorists.

Bibliography

Awan, I., 2017. Cyber-Extremism: Isis and the Power of Social Media. *SOCIAL SCIENCE AND PUBLIC POLICY,* Volume 54, pp. 138-149.

Banks, C., 2016. *Criminal Justice Ethics: theory and practice.* 4th ed. s.l.:SAGE PUBLICATIONS.

Besley, T. & Peters, M. A., 2020. Terrorism, trauma, tolerance: Bearing witness to white supremacist attack on Muslims in Christchurch, New Zealand. *Educational Philosophy and Theory,* 52(2), pp. 109-119.

Blomberg, T. G. & Mastre, J., 2014. Net-Widening. *In The Encyclopedia of Theoretical Criminology.*

Bouhana, N., Corner, E., Gill, P. & Schuurman, B., 2018. Background and Preparatory Behaviours of Right-Wing Extremist Lone Actors: A Comparative Study. *Perspective on Terrorism,* 12(6), pp. 150-163.

Brezina, T., 2017. *Criminology and Criminal Justice: General Strain Theory.* [Online] Available at: https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-249 [Accessed 05 2021].

Bright, J., 2017. *Explaining the Emergence of Echo Chambers on Social Media: The Role of Ideology and Extremism,* s.l.: University of Oxford - Oxford Internet Institute.

Chen, H., Thomas, S. & Fu, T., 2008. Cyber extremism in Web 2.0: An exploratory study of international Jihadist groups. *IEEE International Conference on Intelligence and Security Informatics,* pp. 98-103.

Clemmow, C. et al., 2020. Disaggregating Lone-actor Grievance-fuelled Violence: Comparing Lone-actor Terrorists and Mass Murde. *TERRORISM AND POLITICAL VIOLENCE,* pp. 1-26.

Cohen, B. & Tufail, W., 2017. Prevent and the Normalization of Islamophobia. *Islamophobia: Still a Challenge For Us All.*

Corner, E. & Gill, P., 2015. False Dichotomy? Mental Illness and Lone-Actor Terrorism. *Law and Human Behviour,* 39(1), pp. 23-34.

Costello, M., Hawdon, J., Ratliff, T. & Grantham, T., 2016. Who views online extremism? Individual attributes leading to exposure. *Computers in Human Behavior,* Volume 63, pp. 311-320.

Cottee, S., 2021. Incel (E)motives: Resentment, Shame and Revenge. *Studies in Conflict & Terrorism,* 44(2), pp. 93-114.

Counter Terrorism Policing North East, 2020. [Online] Available at: https://www.hlc-vol.org/wp-content/uploads/2021/03/CTLP-2020-21-NPM.pdf [Accessed 01 05 2021].

Eichhorn, K., 2001. Sites unseen: ethnographic research in a textual community. *Qualitive Studies in Education,* 14(4), pp. 565-578.

Ellis, C. et al., 2016. Analysing the Processes of Lone-Actor Terrorism: Research Findings. *Perspectives on Terrorism,* 10(2), pp. 33-41.

Farwell, J. P., 2014. The Media stratrgy of ISIS. *Survival,* 56(6), pp. 49-55.

Feinberg, J., 1989. *The Moral Limits of Criminal Law.* s.l.:s.n.

Ghani, H. & Nagdee, I., 2019. *The Routledge International Handbook of Islamophobia.* 1st Edition ed. s.l.:Routledge.

Gill, P. & Corner, E., 2016. Lone-Actor Terrorist Target Choice. *Behavioral Sciences and the Law,* Volume 34, pp. 693-705.

Ging, D., 2019. Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere. *Men and Masculinities,* 22(4), pp. 638-657.

Hawdon, J., Bernatzky & Costello, M., 2019. Cyber-Routines, Political Attitudes, and Exposure to Violence-Advocating Online Extremism. *Social Forces,* 98(1), pp. 329-354.

Hitchens, M., Patrickson, B. & Young, S., 2013. Reality and Terror, the First-Person Shooter in Current Day Settings. *Games and Culture,* 9(1), pp. 3-29.

HM Governemnt, 2012. *Counter-Terrorism Local Profiles: An Updated Guide.* [Online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118203/counter-terrorism-local-profiles.pdf
[Accessed 01 05 2021].

HM Governemnt, 2015. *Counter-Extremism Strategy.* [Online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf
[Accessed 24 12 2020].

HM Government, 2020. *Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism.* [Online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/964567/6.6271_HO_HMG_Channel_Duty_Guidance_v14_Web.pdf
[Accessed 01 07 2021].

Hoffman, B., Ware, J. & Shapiro, E., 2020. Assessing the Threat of Incel Violence. *Studies in Conflict & Terrorism,* 43(7), pp. 565-587.

Hollewell, G. F. & Longpré, N., 2021. Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet. *International Journal of Offender Therapy and Comparative Criminology,* pp. 1-18.

Katon, A. et al., 2021. A Qualitative Analysis of Drivers among Military-Affiliated and Civilian Lone Actor Terrorists Inspired by Jihadism. *Studies in Conflicts & Terrorism,* 44(2), pp. 138-155.

Maxwell, D., Robinson, S. R., Williams, J. R. & Keaton, C., 2020. "A Short Story of a Lonely Guy": A Qualitative Thematic Analysis of Involuntary Celibacy Using Reddit. *Sexuality & Culture,* Volume 24, p. 1852–1874.

McGovern, M., 2016. The university, Prevent and cultures of compliance. *Prometheus,* 34(1), pp. 49-62.

Menzie, L., 2020. Stacys, Beckys, and Chads: the construction of femininity and hegemonic masculinity within incel rhetoric. *Psychology & Sexuality.*

Nyamutata, C., 2020. Young Terrorists or Child Soldiers? ISIS Children, International Law and Victimhood. *Journal of Conflict & Security Law ,* 25(2), pp. 237-261.

O'Malley, R. L., Holt, K. & Holt, T. J., 2020. An Exploration of the Involuntary Celibate (Incel) Subculture Online. *Journal of Interpersonal Violence ,* pp. 1-28.

O'Reilley, T., 2009. *What is Web 2.0.* s.l.:O'Reilly Media, Inc..

Regehr, K., 2020. In(cel)doctrination: How technologically facilitated misogyny moves violence off screens and on to streets. *new media & society,* pp. 1-18.

Sage, L., 2015. *Anxiety in The British Media Portrayals of Schoolgirls Heading for Syria,* s.l.: E-International Relations.

Scanlon, J. R. & Gerber, M. S., 2014. Automatic detection of cyber-recruitment by violent extremists. *Security Informatics,* 3(5).

Schmid, A. P., 2013. *Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review,* Hague: International Cenre for Counter Terrorism.

Sotlar, A., 2004. *Some Problems with a Definition and Perception of Extremism within a Society.* [Online]
Available   at: https://www.ncjrs.gov/pdffiles1/nij/Mesko/208033.pdf
[Accessed 24 12 2020].

Vale, G., 2018. *Cubs in the Lions' Den: Indoctrination and Recruitment of Children Within Islamic State Territory,* London: International Centre for the Study of Radicalisation.

Van der Veer, R., 2020. *Analysing personal accounts of perpetrators of incel violence: what do they want   and   who   do   they   target?.*   [Online]
Available   at: https://icct.nl/publication/analysing-personal-accounts-of-perpetrators-of-incel-violence-what-do-they-want-and-who-do-they-target/
[Accessed 13 05 2021].

Van der Vegt, I., Gill, P., Macdonald, S. & Kleinberg, B., 2019. *Shedding Light on Terrorist and Extremist Content Removal,* London: Royal United Services Institute for Defence and Security Studies.

Van Valkenburgh, S. P., 2021. Digesting the Red Pill: Masculinity and Neoliberalism in the Manosphere. *Men and Masculinities,* 24(1), pp. 84-103.

Walker, C. & Cawley, O., 2020. The Juridification of the UK's Counter Terrorism Prevent Policy. *Studies in Conflict & Terrorism.*

Younis, T. & Jadhav, S., 2019. Islamophobia in the National Health Service: anethnography of institutional racism in PREVENT's counter-radicalisation policy. *Sociology of Health & Illness,* 42(3), pp. 610-626.