Online radicalisation: the use of the internet by Islamic State terrorists in the US (2012-2018)

Whittaker, J.J.

Online Radicalisation:

The Use of the Internet by Islamic State Terrorists in the US (2012-2018)

Joe Whittaker

Printing by Ridderprint, the Netherlands

Undertaken as a joint PhD between Universiteit Leiden and Swansea University.

Online Radicalisation

The Use of the Internet by Islamic State Terrorists in the US (2012-2018)

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 19 januari 2022
klokke 11.15 uur

door

Joseph James Whittaker

geboren te Cambridge

in 1988

Promotoren

Prof. dr. E. Bakker

Prof. dr. S. Macdonald (Swansea University, UK)

Co-promotoren

Dr. A. Reed (Swansea University, UK)

Dr. L. Nouri (Swansea University, UK)

Promotiecommissie

Prof. mr. dr. E.R. Muller

Prof. dr. J.A. Koops

Prof. dr. I.G.B.M Duijvesteijn

Prof. dr. P. Gill (University College London, UK)

Dr. B. Schuurman

Dr. G. Weimann

Figures **9**
Tables **10**
Chapter 1: Introduction **13**
1.1 Research Objective 13
1.2 The Growth of Terrorism, the Islamic State, and the Internet 14
1.3 Broad Overview of Knowledge 15
1.4 Online Radicalisation in Policy and the Media 16
1.5 Summary and Originality Claim 17
1.6 A Note on Referencing 18
Chapter 2: The Conceptual Ambiguity of Radicalisation **19**
2.1 Introduction 19
2.2 Conceptual Clarity 19
2.2.1 Definition, Interchangeability, and Derivatives 19
2.2.2 Terrorism 21
2.2.3 Extremism 21
2.2.4 Radicalism 22
2.2.5 End Points: Beliefs versus Behaviour 23
2.2.6 Behaviour 23
2.2.7 Beliefs 25
2.2.7 Combined Definitions 26
2.2.8 Operationalising a Radicalisation Definition 27
2.3 Online Radicalisation: Conceptual Ambiguity 28
2.4 Understanding Radicalisation 30
2.4.1 Models and Theories 30
2.4.2 A Complex Phenomenon 34
2.4.3 Empirical Radicalisation Research – What we know 35
2.5 Conclusion 39
Chapter 3: Online Radicalisation Research **41**
3.1 Introduction 41
3.2 Theorising Online Radicalisation 42
3.2.1 Theories and Dynamics 42
3.2.2 Online Radicalisation Models 45
3.3.3 Ontological Challenges 51
3.3 Two Types of Empirical Research 55
3.4 Demand-Side 56

3.4.1 The Internet is Important 56
3.4.2 Downplaying the Role of the Internet 62
3.5 Supply-Side 67
3.5.1 Islamic State Propaganda Strategy 67
3.5.2 Videos 69
3.5.3 Magazines 70
3.5.4 Twitter 72
3.5.5 Gender 73
3.5.6 Jihadi Cool and Low-Level Content 74
3.5.7 Online Affordances 75
3.5.8 Other Platforms 76
3.5.9 IS Online Post 2016 77
3.6 Conclusion: Locating the Gaps and Research Questions 79
Chapter 4: Methodology 83
4.1 Introduction 83
4.2 Research Design 83
4.3 Data Collection 84
4.3.1 Criminal Justice System 84
4.3.2 Travellers 85
4.3.3 Attackers 86
4.4 Inclusion and Exclusion Criteria 86
4.4.1 Islamic State 87
4.4.2 United States Definition of Terrorism 88
4.4.3 Other Crimes and Terror Enhancements 90
4.4.4 Other Definitions of Terrorism 91
4.4.5 United States of America 92
4.4.6 Dates 92
4.4.7 Exclusion for Insufficient Data 93
4.5 Quantitative Coding 95
4.5.1 Analytic Rationale 95
4.5.2 Accounting for Missing Data 96
4.5.3 Codebook 98
4.6 Analysis 104
4.6.1 Quantitative 104
4.6.2 Grounded Theory 106

4.7 Ethical Considerations 107
4.7.1 Identifying Research Subjects as Terrorists 107
4.7.2 Data Storage 107
4.7.3 Researcher Self-Care 108
4.8 Conclusion 108
Chapter 5: Quantifying the Online Behaviours of Islamic State Terrorists 109
5.1 Introduction 109
5.2 Demographic Snapshot 109
5.3 RQ1: How frequently do terrorists in this sample use the Internet, and in what ways? 117
5.3.1 Online Network Behaviours 118
5.3.2 Social Media Platforms 119
5.3.3 End-to-End Encryption 120
5.3.4 Online Event Behaviours 122
5.3.5 Increase in Internet Usage 123
5.4 RQ2: Has the Internet replaced the offline domain as the primary venue for terrorists' antecedent behaviours? 126
5.4.1 Offline Behaviours - Descriptive 127
5.4.2 Online Network Behaviours versus Offline 128
5.4.3 Online Learning/Planning Behaviours versus Offline 129
5.5 RQ3: Do terrorists that use the Internet exhibit different experiences to those that do not? 130
5.5.1 Event Behaviours – Descriptive 131
5.5.2 Online Network Behaviours versus Event Behaviours 135
5.5.3 Online Learning/Planning Behaviours versus Event Behaviours 136
5.5.4 Number of Co-offenders versus Online Behaviours 136
5.5.5 Age versus Online Behaviours 137
5.5.6 Gender versus Online Behaviours 138
5.6 RQ4: Does using the Internet help or hinder plots? 139
5.6.1 Post Event – Descriptive 139
5.6.2 Post-Event Behaviours versus Online Activity 140
5.6.3 Multivariate – Predicting Event Success 143
5.6.4 Event Success versus Online Network sub-variables 145
5.7 Discussion and Conclusion 146
Chapter 6: The Online Dynamics of Terrorist Pathways 153
6.1 Introduction 153
6.1.2 Grounded Theory 153

6.1.3 Coding 155
6.1.4 Theory Building 156
6.2 The Socialising Role of Radical Content 157
6.2.1 Introduction 157
6.2.2 What Kinds of Radical Content do Terrorists Collect? 158
6.2.3 Links to Plots 163
6.2.4 Socialisation 168
6.2.5 Informal Content 171
6.2.6 Radical Construction 173
6.2.7 Popular Culture 175
6.2.8 Synthesis 177
6.3 Women and Gendered Online Personas 179
6.3.1 Introduction 179
6.3.2 Influencers 180
6.3.3 Peer-to-Peer Communicators 187
6.3.4 Offliners 192
6.3.5 Synthesis 194
6.4 Online Only Trajectories and the Buyers' Market of the Internet 195
6.4.1 Introduction 195
6.4.2 Online Only Trajectories 196
6.4.3 First Steps 203
6.4.4 Synthesis 209
6.5 Conclusion 212
Chapter 7: Discussion 215
7.1 Introduction 215
7.2 Empirical Contribution: The Role of the Internet in Contemporary Terrorist Pathways 215
7.3 Theoretical Contributions 219
7.3.1 Grounded Theory: Radicalisation Dynamics 219
7.3.2 Onlife Radicalisation? 222
7.3.3 Understanding Radicalisation Environments 225
7.3.4 Abdullahi Yusuf and his Environment 227
7.4 Policy Contribution – The Fragile Ecosystem and Unintended Consequences 236
7.5 Limitations 239
7.6 Future Research 240
7.6.1 Theoretical Contributions 241

7.6.2 Sequence Analysis 241
7.6.3 Social Media Affordances 242
7.6.4 The Future 243
Chapter 8: Conclusion 245
8.1 Summary and Key Findings 245
8.2 Informing Policymakers and the Media 247
8.3 Towards an Evidence-based Understanding of Terrorist Pathways 248
Bibliography 251
Academic 251
Statutes Cited 277
Cases Cited 278
Media Sources Cited 286
Acknowledgements 295
Curriculum Vitae 297

Figures

Figure 1 - Radicalisation as a Catch-all Word for Three Different Processes 20
Figure 2 - Saifudeen's (2014) Cyber Orbit Pathway Model 46
Figure 3 - Batug, Douai, & Acka's (2018) Four Step Model of Online Radicalisation 47
Figure 4 - Neo's (2016) RECRO Model 48
Figure 5 - Flowchart of Inclusion/Exclusion Criteria 94
Figure 6 - Age at Event 110
Figure 7 - Occupation 111
Figure 8 - Highest Level of Education 112
Figure 9 - Criminal Record 115
Figure 10 - Type of Mental Health Problem 116
Figure 11 - Date of the Actor's Event 117
Figure 12 - Social Media Platform used by more than 10 actors 120
Figure 13 - Year of Terrorist Event by use of End-to-end Encryption 121
Figure 14 - US Adults' Internet Usage (Pew Research) 124
Figure 15 - Number of Actors Involved in Execution of the Plot 132
Figure 16- Length of Sentence 140
Figure 17 - Author of Radical Content 160
Figure 18 - Radical Content by Terrorist Group 162
Figure 19 - Magazine Series 163
Figure 20 - Ducol's (2016) "Life Spheres" SAT Framework 226
Figure 21 - Yusuf's Online vs Offline Activities 230
Figure 22 - Bouhana's (2019) S5 Inference Framework 231
Figure 23 - Yusuf's 5S Framework 234

Tables

Table 1 - Online Network Behaviours....118
Table 2 - Online Network Behaviours 2....119
Table 3 - Year of Event by Use of End-to-End Encryption....122
Table 4 - Online Event Behaviours....123
Table 5 - Open versus Closed-Source Data....125
Table 6 - Offline Behaviours....127
Table 7 - Offline Network and Online Network Behaviours Significant Correlates....129
Table 8 - Learning and Planning Offline and Learning and Planning Online Significant Correlates....130
Table 9 - Actor's Role in Event....134
Table 10 - Online Network and Event Behaviours Significant Correlates....135
Table 11 - Event Success and Online Behaviours Significant Correlates....141
Table 12 - Known to Security Services and Online Behaviours Significant Correlates....142
Table 13 - Actor Arrested and Online Behaviours Significant Correlates....142
Table 14 - Event Success Logistic Regression: Step 1....144
Table 15 - Event Success Logistic Regression: Step 2....145
Table 16 - Event Success Logistic Regression 2: Online Network Sub-variables....146

Dedicated to all the innocent people that have lost their lives at the hands of terrorism, and the senseless wars against it.

Chapter 1: Introduction

Pathways towards terrorism are complex and multifaceted (Borum 2017; Silva 2018; Hafez and Mullins 2015). However, it is well-documented that humans seek explanations to phenomena that fit a simple narrative which is easy to understand and digest (Kahneman 2012). It is therefore unsurprising that many academics, policymakers, practitioners, and media commentators subscribe to the notion of "online radicalisation," and with it the implication that the Internet plays a causative role in individuals becoming terrorists (Sageman 2008; Weimann 2012; HM Government 2019). This thesis investigates this phenomenon, and then advances the current understanding of terrorists' use of the Internet by empirically analysing the online behaviours of Islamic State (IS) actors in the United States of America. To date, there is little-to-no academic literature which analyses this dataset in the context of the role of the Internet, which is particularly surprising given the repeated affirmation that the group were exceptionally talented at exploiting online platforms with their wide-reaching propaganda (Berger and Morgan 2015; Klausen 2015; Ingram 2015).

1.1 Research Objective

The underlying objective of this thesis is to investigate whether online radicalisation is an analytically useful concept when discussing contemporary cases of terrorism. To do this, it will assess the role of the Internet in contemporary pathways towards terrorism using a mixed methods approach. Chapter 5 utilises a quantitative and (mostly) deductive methodology, asking four research questions which inform this objective:

> *RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?*
>
> *RQ2: Has the Internet replaced the offline domain as the primary venue for terrorists' antecedent behaviours?*
>
> *RQ3: Do terrorists that act online demonstrate different experiences to those that do not?*
>
> *RQ4: Does acting online help or hinder terrorists?*

Chapter 6 investigates the research objective using an inductive analysis inspired by Grounded Theory Methodology (GTM). Rather than seeking to answer existing questions, it discovers emergent themes that are grounded in the data (Glaser and Strauss 1967). This is done by conducting multiple rounds of coding which seek to both capture the phenomenon that is being analysed, as well as articulating relationships by constantly comparing codes in an iterative manner, which are then conceptualised to form theories from the data (Lehane 2017). In this thesis, terrorists' online behaviours are coded in any inductive manner for the purpose of better understanding the dynamics of the role of the Internet in radicalisation pathways. By utilised a mixed method, as well as an inductive and deductive approach, this research offers an important contribution by testing a

number of existing findings within the context of this sample and by providing new theories to be tested in future.

1.2 The Growth of Terrorism, the Islamic State, and the Internet

The events of September 11th 2001 after often seen as a watermark which changed the nature of terrorism. Although many have debated the veracity of this claim, suggesting that much can be learned from old scholarship (Crenshaw 2007), it is clear that in the years proceeding the attack, terrorism quickly rose to the forefront of policy (Lutz and Ulmschneider 2019), media attention (Kellner 2007) and academia (Jackson 2012). The ensuing War on Terror, which led to interventions in Afghanistan and Iraq, framed a large part of the following two decades, and governments have repeatedly affirmed that the fight against terrorism is a policy priority, including the European Council (Council of the European Union nd), the UK (HM Home Office 2018), and the US - with the FBI even claiming that protecting the US from terrorist attacks is the Bureau's number one priority (FBI nd). After the US invasion of Iraq, a terrorist named Abu Musab al-Zarqawi led a militant Sunni resistance against the occupation, which led to the de facto control of the Anbar province before his death by US airstrike in 2006 (Whiteside 2016). Zarqawi had laid the foundation for what would later become IS, via several iterations: Jama'at al-Tawhid wal-Jihad, al-Qaeda (AQ) in Iraq, Mujahideen Shura Council, Islamic State in Iraq, and Islamic State in Iraq and al-Sham (Schmid 2015). The major spark that ignited the group to the forefront of the world's attention was the outbreak of the Syrian civil war in which the Iraq-based group sent a cell east to establish a presence in the conflict (Stern and Berger 2015).

The success of this cell – Jabhat al-Nusra – and military successes in Iraq led to one of the largest mobilisations of foreign terrorist fighters that travelled from around the world to join IS in Syria and Iraq, with estimates totalling between 44,000-52,000 (Cook and Vale 2019). The influx of foreign fighters was described by the UN as one of the gravest threats to international security in its adoption of resolution 2178 (United Nations Security Council 2014). Having established strongholds in Iraq, Syria and elsewhere, the group controlled more than 100,000 km^2 - almost two and a half times the size of the Netherlands – and over 11,000,000 people at its peak in late 2014 (Jones et al. 2017). The group came to worldwide notoriety in 2014 after creating and disseminating a number of gruesome and explicit propaganda videos (for example, see: Winter 2015a), which caught the attention of the global media (Friis 2015). In short, IS became one of the most wide-reaching and dangerous terrorist organisations in history.

At the same time as these developments in the War on Terror and the civil wars in the Middle East, an entirely different type of revolution was taking place – one of communication. The Internet was conceived as a US Government funded project in the 1960s and underwent a number of private iterations before Tim Berners Lee wrote the first web browser, leading to its full commercialisation in 1995 (Bartlett 2015). At this time, there were around 10,000,000 Internet users (Leiner et al. 2009), representing

around 0.2% of the world's population. Today the estimated figure is around 4.47 billion users (Clement 2019) – roughly 57%. An important part of the Internet's success story is the proliferation of mobile data which, via devices such as smart phones and tablets, made the Internet accessible almost anywhere. Furthermore, social media platforms such as Facebook, Twitter, and YouTube, which prioritised peer-to-peer networking and audio-visual technologies, have become ubiquitous, with over 2.82 billion using such platforms in 2018 (Statistica 2019). The Internet and social media has completely transformed day-to-day life, fundamentally changing political discourse (Polat 2005; Rowe 2015), entertainment (Gomez-Uribe and Hunt 2015; Lewis et al. 2005), and commercial activities such as shopping (Pantano et al. 2016). In short, in the space of 25 years, online became the new norm.

Given the ubiquity of the Internet it should, perhaps, not be surprising that terrorists have also turned to the Web. Many scholars have argued that terrorists have typically been early adopters of new technologies to communicate and recruit (UN CTED 2015; Levin 2015; Bloom et al. 2017). Indeed, Zarqawi himself was Internet savvy, uploading several videos for the purposes of building a brand and amplifying his brutal violence in 2004 (Conway 2012). Through the 2000s, jihadists utilised online fora to communicate and spread propaganda (Hegghammer 2014; Torres-Soriano 2016), as well as chat rooms, email, and websites (Sageman 2008a). However, the rise of IS, which took place concurrently with the growth of social media, was more than the mere adoption of online platforms. Rather, their online propaganda strategy has been frequently described as sophisticated (Zelin 2015; Winter 2015b) and their output quality as "Hollywood-esque" (Winter 2018; Cook and Vale 2018). The group had a substantial reach on social media, potentially as large as 90,000 sympathetic accounts on Twitter (Berger and Morgan 2015) with the foreign fighters documenting their life in the caliphate in real time, sending the information around the world to onlookers (Carter et al. 2014; Klausen 2015).

1.3 Broad Overview of Knowledge

The widespread use of the Internet and social media platforms by terrorist organisations led to the emergence of the concept of online radicalisation. Although a fundamentally nebulous and ill-defined concept (Gill et al. 2015; Meleagrou-Hitchens and Kaderbhai 2017; Macdonald and Whittaker 2019), it was frequently posited that the Internet was playing a more prominent role in individual pathways towards terrorism, with some even claiming that 'face-to-face radicalization has been replaced by online radicalization' (Sageman 2008b, p.41). At the same time, the notion of the "lone wolf" emerged, who radicalises alone on the Internet without the traditional group structures of a terrorist organisation (Weimann 2012). Individual cases began to emerge, like that of Roshonara Choudhry who attempted to murder British Member of Parliament Stephen Timms in 2010, who supposedly "self-radicalised" via the Internet without any apparent offline connections (Pearson 2016), or Jake Bilardi, a seventeen year-old who left his native Australia for Syria having conducted extensive online "research" and was not part of any

radical offline social networks (Cook and Vale 2018; Whittaker 2018). In these instances, it is easy to see how the idea of online radicalisation became widespread; individuals seemingly acted entirely in the online domain until the moment that they conducted their act of terror. Moreover, given the nature of IS' communication campaign, which was both sophisticated and far away from potential recruits, many have suggested that the phenomenon was at least partly responsible for both the flow of foreign fighters and those that conduct terror attacks in their country of origin (UN CTED 2015; Koehler 2014).

Despite the notion of online radicalisation becoming prevalent in recent years, the empirical evidence for this phenomenon has been less clear. It is apparent that terrorists do use the Internet heavily for a number of different purposes including online communication, accessing propaganda, and planning their events (Bastug et al. 2018; Gill et al. 2017; von Behr et al. 2013). However, research has also highlighted the importance of face-to-face communication, while also suggesting that "online only" pathways towards terrorism are rare (Gill et al. 2017; Reynolds and Hafez 2017; von Behr et al. 2013). Rather, in the majority of instances, offline networks and interactions seem to still be central. Importantly, qualitative research has suggested that the Internet may provide a space for, and even reward, terrorists' construction of a radical identity that may not be possible offline (Pearson 2016; Koehler 2014; Brachman and Levine 2011). These two sets of findings offer different perspectives on the role of the Internet in terrorism, with the former somewhat downplaying its importance – at least in the context of other factors – and the latter suggesting that it may play a crucial role. However, there is still a substantial dearth of empirical research into this phenomenon; studies of terrorism online tend to focus heavily on the material that individuals can find online and there are few which focus on the pathways of terrorists (Gill et al. 2015; von Behr et al. 2013).

1.4 Online Radicalisation in Policy and the Media

Countering online radicalisation has become a policy priority for almost every country and international institution. Europol note that online propaganda and networking are essential to terrorists' attempts to radicalise European audiences (Europol 2018). The UK Government's *Online Harms White Paper* takes a similar tone, noting that 'terrorist groups use the internet to spread propaganda designed to radicalise vulnerable people' (HM Government 2019, p.5). In 2017, British Prime Minister Theresa May and French President Emmanuel Macron established a joint UK-France initiative to tackle online radicalisation, including stronger regulations against tech companies that fail to remove terrorist content (HM Government 2017), which was endorsed by Dutch Prime Minister Mark Rutte, who claimed that it was necessary to stop 'vulnerable young people from being exposed to terrorist ideologies on their smartphones and laptops and being drawn in' (Rutte 2017). The EU Council also highlight the danger of online radicalisation, vowing to counter it using a number of methods including disruption of terrorists' use of the Internet and by challenging groups' ideologies (Council of the European Union 2014). Across the Atlantic, the FBI emphasise the danger too, suggesting that terrorists often

radicalise online and mobilise to violence quickly (FBI nd), while the Obama administration responded to the threat posed to Americans by creating the "Interagency Working Group to Counter Online Radicalization to Violence" to promote Internet safety (Wiktorowicz 2013). At the UN level, former Secretary General Ban Ki-Moon told the Security Council that it was critical to halt the exploitation of social media by terrorists, which was being used to radicalise foreign fighters to join IS in Iraq and Syria (Ki-Moon 2016).

Despite a lack of empirical support for online radicalisation as a widespread phenomenon, it is often represented that way within the media. Both during the rise of IS and the resurgence of the far-right, it has become common to see headlines such as: 'How Online Radicalization Is Drawing Young Western Women to the Islamic State' (Al-Jezairy 2015), 'We Need to Talk About the Online Radicalisation of Young, White Men' (Wilkinson 2016), or 'The New Radicalisation of the Internet' (New York Times Editorial Board 2018). Frequently, journalists seem to give radicalising agency to the Internet, for example, articles which refer to "YouTube, the Great Radicalizer", while outlining the dangers of social media platforms and ways in which their affordances may drive the process (Tufekci 2018). While it is not uncommon for phrases to be appropriated by editors for the purposes of selling newspapers or generating clicks, it is clear that online radicalisation has cemented itself in contemporary Western popular culture.

1.5 Summary and Originality Claim

The motivation for this research was born out of the context presented above. Terrorists clearly use the Internet to attempt to recruit new members and fortify the beliefs of those that have already accepted their ideology. Moreover, in the years that led up to the beginning of this research, policymakers, the media, and public intellectuals were diagnosing the largest mobilisation of foreign fighters in history and a number of large-scale terrorist attacks as the result of online radicalisation. However, it has never been clear to me what – exactly – the phrase means and the empirical research does not suggest that it is a widespread phenomenon. However, when the project began, there had been little-to-no systematic research studying whether IS terrorists had radicalised online. It is possible that the group's wide-reaching and sophisticated propaganda strategy played a driving role in individuals' pathways towards terrorism, or that the world's ever-greater reliance on the Internet had shifted the process from the offline to the online domain. As such, an empirical investigation into the role of the Internet in terrorists' pathways is necessary. This thesis' claim to originality is threefold. Firstly, there are still few studies which analyse terrorists' use of the Internet by looking at the pathways of individual actors; secondly, and relatedly, it is the first to do this by studying the cohort of IS terrorists in the US; and finally, it uses these empirical findings to make important theoretical contributions to the idea of "online radicalisation."

What follows below seeks to empirically unpack the concept of "online radicalisation," studying the online behaviours of 201 IS actors within the US. Chapter 2 focuses on the

conceptual issues surrounding the process of radicalisation more broadly, including definitional problems, theoretical models, and the state of research. Chapter 3 surveys the existing literature on online radicalisation, first discussing theoretical research before reviewing the "demand" side of the field – i.e. how individual terrorists or extremists use the Internet – and then assessing the research into the "supply" of IS material online. Chapter 4 lays out the methodological considerations for the thesis, narrowing the focus from the nebulous concept of online radicalisation to analysing the observable behaviours of terrorist actors. It outlines the research design, methods of data collection, inclusion and exclusion criteria, coding system, methods of analyses, as well as ethical considerations.

Chapter 5 is a quantitative analysis of the sample, first looking at the demographics of the cohort before answering the four research questions laid out above. Although terrorists use the Internet heavily as part of their trajectories, there is little reason to believe that the online domain has replaced offline. In fact, there is good reason to believe that acting online may hamper would-be terrorists' opportunities to conduct their plots. Chapter 6 employs a mixed methods GTM approach to establish emergent themes within the data, offering three radicalisation dynamics: Firstly, that consumption of propaganda should be seen as part of an ongoing socialised radicalisation process; rather than consuming content in a unidirectional manner, terrorists discuss, share, and create new content. Secondly, the Internet may offer females a space to construct a radical identity free of the constraints that may exist in offline jihadist networks, and finally, that the abundance of information on the Internet is a "buyers' market" for radicalising individuals, who can gratify their specific needs. Chapter 7 synthesises the findings into the contributions of the thesis at the empirical, theoretical, and policy level.

This research is not confined to a singular ontological or epistemological lens. It is primarily focused on behaviours, which lends itself to a realist/positivist understanding which assumes that data are real, observable, and knowable. This is particularly prescient in the quantitative and statistical analysis. However, some of the inductive findings of the GTM chapter offer a constructivist viewpoint relating to the ongoing social relationships of terrorists, focusing in particular in how individuals form identities in the online sphere.

1.6 A Note on Referencing

This thesis employs a slightly unusual referencing style. When discussing the academic literature, it follows the Harvard 9th Edition. However, when referencing a data point as evidence, mostly in Chapters 5 and 6, it employs the Oxford-style footnotes system. It was deemed worthwhile to demarcate these types of reference so the reader could easily understand when the thesis was making an argument in relation to the literature and when it was providing support from the dataset. Moreover, particularly in Chapter 6, the triangulation of data from several different sources would render the chapter almost unreadable if it were to use in-text referencing. What follows is, I believe, the clearest way to present the data to the reader.

Chapter 2: The Conceptual Ambiguity of Radicalisation

2.1 Introduction

Before moving to a discussion of the role of the Internet in radicalisation, it is first prudent to conceptually investigate what is meant by "radicalisation". There is a considerable ambiguity surrounding the deployment of the word. It is usually used to mean a process towards one of three end points: becoming a terrorist, an extremist, or a radical. These end points are not causally related and each can have substantially different normative connotations, which further exacerbate the lack of conceptual clarity. At the heart of this ambiguity is a disagreement as to whether radicalisation is a cognitive or behavioural phenomenon – that is to say, whether the process is complete with the adoption of a set of beliefs, or whether a specific behaviour must be undertaken. This thesis adopts a working definition of radicalisation that focused on terrorists' antecedent behaviours. The chapter then moves on to ambiguities that are inherent to the concept of "online radicalisation," questioning what role the Internet must play for a terrorist to be deemed to have radicalised online.

This chapter then moves to research which attempts to theorise and model the process of radicalisation, finding that many of these attempts have fallen short, relying on unsystematic evidence and not lending themselves to empirical testing. It then gives an overview of the existing empirical evidence into common factors in radicalisation including age, gender, socioeconomic factors, education, environment, the role of converts, criminal experiences, and mental health. While attempts to profile terrorism have tended to fail, there are some commonalities that may be associated with radicalisation, even if they are neither necessary or sufficient.

2.2 Conceptual Clarity

2.2.1 Definition, Interchangeability, and Derivatives

One of the problems pertaining to the study of radicalisation is the number of conceptual disagreements which ultimately make defining the term difficult. When the word is used, it can be in relation to the process in which an individual comes to engage in terrorism, extremism, or radicalism. This divergence of definitions means that there is a debate regarding the end point of radicalisation; whether one is radicalised towards extreme beliefs or extreme actions.

Despite the conceptual differences, there is one universal point of agreement – radicalisation is a process; the nature of the suffix of the word – *isation* – implies a specific event happening, from before to afterwards. Just as the word "homogenisation" refers to the process of two or more separate things becoming similar or identical, "radicalisation" undeniably refers to a process (For example, see: Gartenstein-Ross and Grossman 2009; Borum 2011; Helfstein 2012; Canetti et al. 2013; Doosje et al. 2016). Importantly, neither

of the words that are most often associated in common parlance with radicalisation – terrorism and extremism – carry the same suffix, nor do they have derivative words that denote a process.[1] There is no "extremisation" and "terrorisation" does not denote the process of becoming a terrorist. Although this may seem like a semantic triviality, the lack of appropriate *isation* suffix results in the term radicalisation becoming a catch-all word for the process towards terrorism and extremism, which has compounded many of the conceptual difficulties, as can be seen in Figure 1.

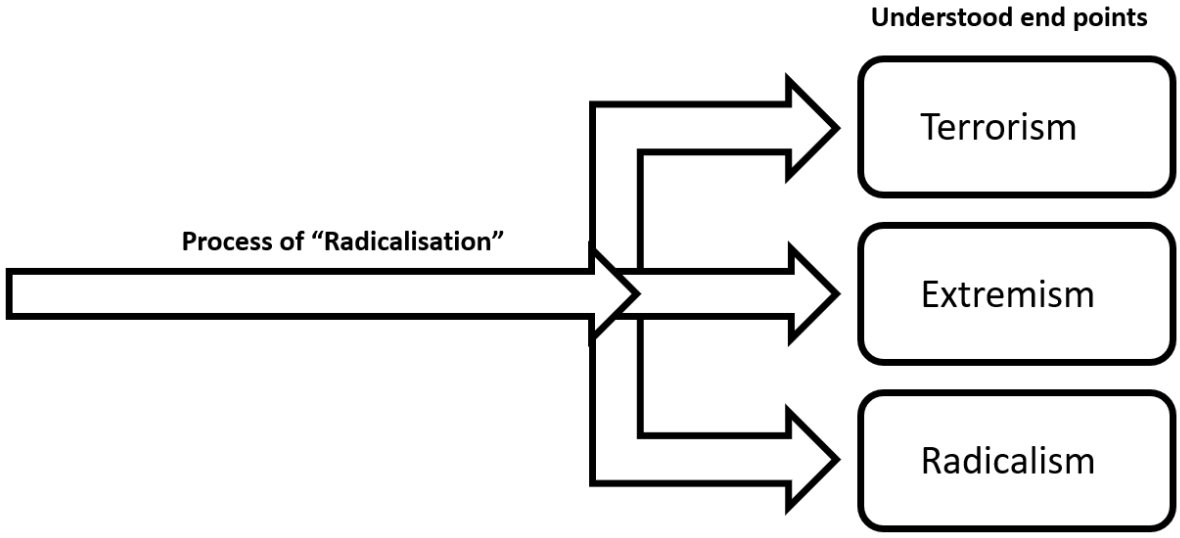


Figure 1 - Radicalisation as a Catch-all Word for Three Different Processes

Although scholars agree that radicalisation denotes a process, there is little consensus on what the process actually leads towards. The obvious semantic choice, radical or radicalism, is used sparingly (Schmid 2013; Bartlett and Miller 2012; Snow and Cross 2011; Borum 2011a). Many scholars will define it by the accumulation of extremist beliefs (Helfstein 2012; McCauley and Moskalenko 2008; Berger 2017; Powers 2014). This can be seen in practice too; the 2015 UK Prevent Strategy review defines radicalisation as 'the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups' (HM Home Office 2015, p.21). Similarly, Hunter and Heinke (2011) note that the FBI defines it as 'the process by which individuals come to believe their engagement in or facilitation of nonstate violence to achieve social and political change is necessary and justified' (Hunter and Heinke 2011). The majority, however, define it simply as a precursor to terrorism or political violence, often having previously adopted extreme beliefs (Klausen et al. 2016; Doosje et al. 2016; Silber and Bhatt 2007; Moghaddam 2005; Lygre et al. 2011; Leistedt 2016; Pettinger 2015; Vidino et al. 2017; Venhaus 2010; Webber and Kruglanski 2017). It is a fair characterisation, as Sedgwick explains, that the word '"radicalization" is for the most part, the term used to describe "what goes on before the bomb goes off"' (Sedgwick 2010). There is nothing inherently wrong with redefining terms to fit a new contextual purpose (this is a

[1] The word "jihadization" has been used in one widely-cited piece of research, but is not used in the bulk of the literature (Silber and Bhatt 2007).

pervasive function of language), however, in this instance, it has resulted in a lack of clarity over the meaning of the word.

2.2.2 Terrorism

To make matters more complicated, the three words most associated with radicalisation – terrorism, extremism, and radicalism – are fundamentally contested in themselves. It is not the author's intent to revisit the long debate on the definition of terrorism, but suffice to say:

> Academics, politicians, security experts and journalists all use a variety of definitions of terrorism. Some focus on the terrorist organizations' mode of operation. Others emphasize the motivations and characteristics of terrorism (Ganor 2002, p.290)

The wide berth of definitions tends to, as Schmid observes, fulfil the interests of the power holders in the domestic and international political systems who have "defining agency" (Schmid 2004). Schmidt is suggesting that because the powerful are able to define terrorism, they invariably use this definition to fulfil their political goals, particularly because it is normative, conjuring up emotive images. A central thesis of critical terrorism studies is that this is problematic because the terrorist actions of states are ignored because common definitions, usually created by states themselves, exclude them (Stohl 2008). This debate has largely resulted in a stalemate; there continues to be no universal definition of terrorism and different states have vastly different "designation lists" (Meserole and Byman 2019). Some scholars, like Ramsay (2015) have argued that it is better undefined because of the heterogeneity of contexts in which the word is used, suggesting it is a "hollow concept". In short, there are many that contest both the definition of the word and the normative manner in which it is deployed.

2.2.3 Extremism

Attempts to define extremism are equally difficult, as the UK Government's 2015 Prevent Guidelines show:

> Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas (HM Home Office 2015, p.21)

The UK definition bears a stark contrast to some academic definitions, such as that of Berger: 'A spectrum of beliefs in which an in-group's success is inseparable from negative acts against an out-group. Negative acts can include verbal attacks and diminishment, discriminatory behaviour, or violence' (Berger 2017, p.6) or Schmid's definition: 'extremists strive to create a homogeneous society based on rigid, dogmatic ideological tenets; they seek to make society conformist by suppressing all opposition and subjugating minorities' (Schmid 2013, p.9).

It is clear that such definitions are fit for the purpose they serve; a lawmaker or practitioner may have little use for a definition that requires analysis of the interplay between an in-group and out-group, while the academic may deride the notion of "fundamental British values" as a political tool (Poole 2016). However, it is clear that, as for the definition of terrorism, there is no commonly accepted term of extremism. Much debate around the definition focuses on the difference between violent (which includes terrorism) and non-violent extremism, as Richards argues: 'if we are to engage with the concept of extremism…a clearer distinction needs to be made between extremism of (nonviolent) thought and extremism of method' (Richards 2015, p.376). The recently created UK Commission for Countering Extremism highlights the lack of consensus around the word and that it is prudent to treat violent extremism as separate to hateful extremism as the two require markedly different strategies (Commission for Countering Extremism 2019). This mirrors much of the debate regarding radicalisation; lending further weight to the notion that radicalisation has become a catch-all term for the process of extremism.

2.2.4 Radicalism

The less-used end-point, radicalism, is also unclear and contested. Although it is sometimes used more-or-less interchangeably with terrorism and extremism (Kruglanski et al. 2014; LaFree 2017; Hafez and Mullins 2015), it is also used when authors are making a point regarding the problematic nature of conflating those two words with radicalisation (Schmid 2013; Bartlett and Miller 2012; Borum 2011a). Bartlett (2017) describes radicals simply as those that advocate fundamental social or political reform, while Snow and Cross (2011) argue that sociological understandings of the term are often vague because radicals are often defined by their context. They offer the following definition: 'a social movement activist who embraces direct action and high-risk options, often including violence against others, to achieve a stated goal' (Snow and Cross 2011, p.118).

Schmid concurs with Snow and Cross's argument, noting that the 'content of the concept 'radical' has changed quite dramatically in little more than a century…[and] we must conclude…that 'radical' is a relative concept' (Schmid 2013). He suggests that it ought to be defined by two main elements:

1. Advocating sweeping political change, based on a conviction that the status quo is unacceptable while at the same time fundamentally different alternatives appears to be available to the radical;
2. The means advocated to bring about the system-transforming radical solution for government and society can be non-violent and democratic (through persuasion and reform) or violent and non-democratic (through coercion and revolution) (Schmid 2013, p.8)

Schmid distinguishes this from his aforementioned definition of extremism, suggesting that the two should be considered quite separate. Snow and Cross and Schmid both agree

that there is a high degree of relativism when the term is used in common parlance, before cementing that point by offering quite different definitions of the term (such as the necessary condition of risk taking and direct action).

It should be clear, even before analysing the word "radicalisation," that there is a lack of clarity due to the words that are associated and often used interchangeably with it. When one uses the term, it is unclear whether it is in relation to terrorism, extremism, or radicalism. This is important because, as Schuurman and Taylor (2018) argue, these are three distinct concepts which are not causally related. All three words are contested and ambiguous themselves, creating two tiers of confusion. Moreover, the three words all have different normative connotations which affect their understanding, which in turn affect the conceptual clarity of the word "radicalisation" itself; to refer to the radicalisation process of becoming a terrorist has clear negative connotations which are not shared if one is referring to the process of becoming a radical.

2.2.5 End Points: Beliefs versus Behaviour

The conceptual difference at the heart of this ambiguity is whether radicalisation is a cognitive or behavioural process. As noted above, there is an academic consensus that radicalisation represents a process, but little agreement on what the end of the process looks like. Neumann argues that research in the field of radicalisation studies is divided into two ends: a cognitive phenomenon in which actors adopt extreme *beliefs* or those who focus on extreme *behaviour* (Neumann 2013b). This relates to the confusion regarding interchangeable words. Those that research radicalisation as the route to terrorism are purporting a version of behavioural radicalisation, while those who use it interchangeably with extremism and radicalism are generally focusing on beliefs as the end result. Of course, many definitions of extremism suggest that such belief *may* result in political violence, like the above definition of Berger (2017). However, the point at which the radicalisation process is complete hinges on the change in belief, not behaviour. Conversely, behavioural radicals may well adopt extremist beliefs, but their process is not complete until it manifests in some kind of action.

2.2.6 Behaviour

The most commonly-held understanding of radicalisation, as noted above by the connection with the term terrorism, is in connection with committing violent acts. Of course, not *any* violent act will suffice; nobody discusses those convicted of homicide as having been radicalised. There must be an ideological element to the behaviour. A report by the New York Police Department defines radicalisation as: 'the progression of searching, finding, adopting, nurturing, and developing this extreme belief system to the point where it acts as a catalyst for a terrorist act' (Silber and Bhatt 2007, p. 16). It is not only the final act of terrorism, but that it is motivated by an extreme belief system. Similarly, Jenkins defines radicalisation as:

> The term "radical" applies to one who carries his theories or convictions to their furthest application. It implies not only extreme beliefs, but extreme action.

> Radicalization refers to the process of adopting for oneself or inculcating in others a commitment not only to a system of beliefs, but to their imposition on the rest of society (Jenkins, Forward to: Gartenstein-Ross and Grossman 2009, p.7)

Again, it is a necessary condition that the 'radical' has extreme beliefs, but not sufficient. On these readings, sufficiency can only obtain when these beliefs are put into action. This type of definition is common in widely-cited research (For example, see: McCauley and Moskalenko 2008; Helfstein 2012; Klausen et al. 2016).

There are many scholars who argue for a stricter demarcation between cognitive and behavioural radicalisation, suggesting that trying to identify and police beliefs is misguided and that the problematic element – behaviour – should be the primary focus. Richards notes that 'counterterrorism, rather than focusing on the threat from terrorism, has itself become increasingly ideological – it has gone beyond the remit of countering terrorism and has ventured into the broader realm of tackling ideological threats to the state' (Richards 2015, p.380). This point is also made by Borum, who argues that understanding radicalisation as developing beliefs as a precursor to terrorism is flawed, observing that 'most radicals did not (and do not) engage in terrorism, and many terrorists did not (and do not) "radicalize" in any traditional sense' (Borum 2011c, p.2). The fundamental point that both Richards and Borum are making is that 'conflating the two concepts undermines our ability to effectively counter either of them' (Borum 2011c, p.2). On this reading, it is clearly the case that ideology and beliefs play an important role in the route to violent extremism, but there are many other factors, including predisposing life experiences, activating situations, predisposing vulnerabilities, and social and group dynamics (Borum 2017). To avoid confusion with behavioural radicalisation, Borum suggests referring to this as an "action pathway" (Borum 2011c) – also called "terrorist pathways" by Horgan (2008) – although referring to it as "radicalisation" is still pervasive in the literature.

However, this dichotomy, according to Neumann (2013b), is a false one, suggesting that the detractors of cognitive radicalisation, such as Borum, have created a straw man:

> The notion of a 'unidirectional relationship' between beliefs and terrorism may exist in the minds of some right-wing bloggers, but it has never gained traction among members of the scholarly community. None of the widely used models and theories of radicalization suggest that beliefs or ideologies are the sole influence on or explanation for why people turn to terrorism (Neumann 2013b, pp.879-880).

Neumann accepts the fact that not all cognitive extremists become terrorists and that not all terrorists are extremists, but this causes Borum to assume that beliefs are overrated in understanding behavioural radicalization. Rather than beliefs being just "one of many" factors, Neumann argues that the behaviour of the IRA compared to the peaceful Tibetans, or the 'quietist' Salafists compared to Al-Qaeda 'can only be understood by looking at, among other factors, the different strands of their belief system and what they

say about the circumstances in which violence is permitted…Without reference to beliefs, none of these behaviours make any sense' (Neumann 2013b, p.880). He concludes that for academia to derive a better understanding of behavioural radicalisation, more, rather than less, effort should be spent attempting to understand beliefs. This position correctly identifies that the separation of beliefs from behaviour does not, as Borum suggests, offer a "clearer picture" into how individuals radicalise behaviourally. Instead, it restricts understanding of how beliefs may foster (or not foster) violent behaviour.

2.2.7 Beliefs

Scholars like Neumann (2013b) argue that it is not desirable to separate beliefs from behavioural radicalisation. However, it may be desirable to do the converse: separate behaviour from cognitive radicalisation – at least by way of an end result. Christmann (2012) argues that the growing synonymy between terrorism and radicalisation introduces a systemic bias towards 'that smaller cohort of individuals who, once radicalised, go on to commit acts of violence…[and] away from the radicalisation process that proceeds terrorism' (Christmann 2012, p.4). Christmann takes the view that radicalisation ought to be defined by the adoption of extreme beliefs and that focusing on terrorism and political violence neglects those who hold similar beliefs but choose not to act on them. The idea of a systematic bias can also be seen in Bartlett and Miller (2012), who compare a group of nonviolent radicals to assess the differences between them and those who do turn to violence. Of course, this method fuses definitions of both cognitive and behavioural radicalisation to some extent because it assesses them against each other, but to do so, one must first accept that behaviour as a necessary and sufficient condition for radicalisation is flawed.

However, there is a contention concerning the *type* of belief that is sufficient for cognitive radicalisation: extremist or radical. Radicalisation to extremism, at its most simple is "the process of developing extremist ideologies and beliefs'[2] (Borum 2011, p.9). The above quoted UK Prevent and FBI definitions of radicalisation focus on the *support* of violence and extremist ideologies (HM Home Office 2015; Hunter and Heinke 2011). Berger offers a different, and slightly more nuanced definition:

> The escalation of an in-group's extremist orientation through the endorsement of increasingly harmful actions against an out-group or out-groups (usually correlating to the adoption of increasingly negative views of the same) (Berger 2017, p.7)

All four definitions have two important things in common. Firstly, as noted above, they relate to beliefs rather than behaviour. Of course, such beliefs *may* be conducive to behaviour (notably violence), but the process of radicalisation is complete when beliefs change. Secondly, the beliefs themselves are deemed to be, either implicitly or explicitly, normatively bad – the use of the word "extremist" often manufactures this judgement,

[2] For Borum, as noted above, this is different to radicalisation to terrorism, for which he emphasises a strong demarcation. He calls this an 'action pathway'.

but also references to the support of violence or harmful actions. Clearly, when one refers to radicalisation in this context, it is condemning the development of unhealthy beliefs that may lead to harmful behaviour.

Not all researchers share this notion of normative radicalisation though. Some scholars use the term "radical" or "radicalism" to distinguish between radicalisation that leads to terrorism or extremism, by using a normative-neutral understanding of the term. Bartlett and Miller (2012), for example define it as:

> The process by which individuals are introduced to an overtly ideological message and belief system that encourages movement from moderate, mainstream beliefs towards extreme views. To be a radical is to reject the status quo, but not necessarily in a violent or even problematic manner (Bartlett and Miller 2012, p.2).

Schmid concurs with this notion, arguing that one must separate radicalism from extremism to 'keep the concept analytically useful and not just a political container term used by political players' (Schmid 2013, p.7). Rather, in many contexts, such as in America, 'the very idea of 'radicalism' has positive connotations…Radicals are an essential part of their national story' (Neumann 2013b, pp. 876-877). While radicalising to become an extremist is clearly understood as normatively bad, doing so to become a radical is anywhere on the spectrum of bad to neutral to good.

2.2.7 Combined Definitions

A final category of definition of radicalisation is one that incorporates both cognitive and behavioural elements. Schmid offers an example of this in his extensive "re-conceptualisation" of radicalisation, which is created from a literature review of existing definitions:

> An individual or collective (group) process whereby, usually in a situation of political polarisation, normal practices of dialogue, compromise and tolerance between political actors and groups with diverging interests are abandoned by one or both sides in a conflict dyad in favour of a growing commitment to engage in confrontational tactics of conflict-waging. These can include either (i) the use of (non-violent) pressure and coercion, (ii) various forms of political violence other than terrorism, or (iii) acts of violent extremism in the form of terrorism and war crimes. The process is, on the side of rebel factions, generally accompanied by an ideological socialization away from mainstream or status quo-oriented positions towards more radical or extreme positions involving a dichotomous world view and the acceptance of an alternative focal point of political mobilization outside the dominant political order as the existing system is no longer recognized as appropriate or legitimate. (Schmid 2013, p.18)

This conceptualisation relies on several contingencies (use of words such as "usually," "generally," and "can include"), which offer a more nuanced descriptive understanding,

but the lack of necessary conditions offers a poorer definitional understanding. The only part of this definition that *must* occur for radicalisation is the breakdown of dialogue, compromise, and tolerance between political actors and groups and a growing commitment for confrontational tactics. These conditions include both behavioural (the breakdown of dialogue and compromise) and cognitive (breakdown of tolerance and commitment for confrontation) aspects. This approach is similar to Fletcher's (2006) "family-likeness" approach to defining terrorism; he argues that terrorism is made up of eight different factors, but not all necessarily apply at the same time and, as such, consist of overlapping factors. While Schmid's definition seems to bridge the gap between the two understandings, it is difficult to see how this could be operationalised systematically for empirical research.

2.2.8 Operationalising a Radicalisation Definition

It should be clear that there is a substantial degree of conceptual ambiguity surrounding the definition of radicalisation. The term can be used to describe the three different processes which are not causally related (Schuurman and Taylor 2018). These processes denote one of two different end points – radical beliefs or radical behaviour. This is not a trivial distinction; one cannot necessarily discern if it means the process of becoming a terrorist, a non-violent extremist, or a radical who is trying to change the world for the better. Moreover, the normative and political nature of each of these understandings makes it even cloudier. Schmid (2013) argues that: 'With such heterogeneous definitions, it is hard to conclude otherwise that 'radicalisation' is a very problematic concept' (Schmid 2013 p.6). It is important for such concepts to be clear for the robustness of research:

> Flitting between different understandings of the abstract concept could result in some variables representing understanding X, other representing understanding Y and still other representing understanding Z. The result will be a flawed measurement of the abstract concept. (Macdonald and Whittaker 2019, p.34)

To simply use the word "radicalisation" without being sufficiently clear about the meaning runs the risk of conducting misleading research. Moreover, it affects the ability of others to synthesise this research for the purposes of meta-reviews as well as the ability of the research to convey their findings to interested parties such as policymakers and the media (Macdonald and Whittaker 2019).

Schuurman and Taylor (2018) argue that there is a "specificity gap" in the common understanding of radicalisation because it conflates adoption of extreme beliefs with extreme actions, while leaving other, equally important, factors unemphasised; they suggest the word "fanaticism" is a better framework for understanding the relationship between beliefs and actions. McCauley and Moskalenko (2017), who accept this misconception, disagree. They argue that, even if conceptually ambiguous, getting rid of words like "radicalisation" and "extremism" will not fix the problem because new names will appear to denote the same process. Instead, they argue that specificity is the answer,

following the lead of Borum (2011c), in separating trajectories towards violence (calling them "action pathways") and those to extremism. They are both right, specificity is clearly the answer to this ambiguity.

When describing the study of radicalisation in 2010, Githens-Mazer and Lambert were damning, arguing that it was a research topic 'plagued by assumption and intuition, unhappily dominated by 'conventional wisdom' rather than systematic scientific and empirically based research' (Githens-Mazer and Lambert 2010, p.889). As will be discussed below, the field is no longer in such a poor state, in large part because it has embraced specificity within research. For example, there are several studies which, using primary or secondary data, analyse discrete, identifiable behaviours as part of terrorists' trajectories (For example, see: Gill et al. 2017; Corner, Bouhana and Gill 2018; Klausen et al. 2018; Lafree et al. 2018; Schuurman et al. 2018). Furthermore, studies that seek to experimentally test factors identified above are specific in their hypotheses and findings as they relates to beliefs or behaviour (Canetti et al. 2013; Federico et al. 2013; Webber et al. 2018). Even though the word "radicalisation" is still pervasive within the field of research, it has adapted to a place that is no longer as Githens-Mazer and Lambert (2010) described it.

With all sides of the radicalisation end-point debate in mind, a working definition is required to empirically study this topic. This thesis will draw from the behavioural understanding of the concept: i.e. *the process of engaging in terrorism or violent extremist actions* (Horgan 2008; Borum 2011a; Klausen et al. 2016). Horgan and Borum suggests calling this a 'terrorist pathway' or 'action pathway' (respectively) to demarcate from radicalisation of beliefs. However, given that this research is attempting to better understand the process of "online radicalisation," it is better to define the concept under investigation and be clear about how it will be treated. It is worth noting that this does not suggest ideology is irrelevant – to become radicalised under this definition an individual must commit an ideological act (i.e. terrorism or violent extremism) – this will be further explained in Chapter 4. However, the change in ideology is not considered the end point of the process, as others have defined it (e.g. Berger 2017).

2.3 ***Online Radicalisation: Conceptual Ambiguity***

As well as the conceptual issues surrounding the deployment of the word "radicalisation," there are also a number of ambiguities in the phrase "online radicalisation." In their review of the literature on this topic Meleagrou-Hitchens and Kaderbhai note that: 'As with the wider debate on radicalisation, there is little agreement on what constitutes online radicalisation and how, if at all, it happens' (Meleagrou-Hitchens and Kaderbhai 2017, p.17). Similarly, in conducting a review of news sources before their empirical study on UK-based terrorists, Gill et al. (2015) highlight that the term is frequently deployed to mean different things:

> One of the key problems is an abundance of conceptual problems. A wide-range of virtual behaviours is subsumed into the category of online radicalisation. A simple search of news articles from March 2015 shows that a range of behaviours from accessing information on overseas events via the Internet, to accessing extremist content and propaganda, to detailing attack plans in a blog post, have all been considered as online radicalisation (Gill et al. 2015, p. 5).

In essence, they are suggesting that displaying any number of online behaviours related to terrorism in the online domain is sufficient to be deemed "online radicalisation." They also note that although academics have tried to remedy this problem with more specificity, none have been successful in quantifying the regularity of the behaviours (Gill et al. 2015). Von Behr et al's (2013) study conducts a review of the available literature to discern five hypotheses of online radicalisation with which to test against their sample. This will be discussed in more detail below, but again, it suggests a number of behaviours which can be conceptualised as online radicalisation.

This problem is also identified by Macdonald and Whittaker (2019), who conduct a literature search for sources which research online radicalisation, finding that only 21% defined the phrase when using it. Pertinently, for those that did define it, the definition diverged from others in important ways which affect the judgement of whether individuals radicalised online or not (Macdonald and Whittaker 2019). For those that do not define the term, one can, at best, infer a definition or understanding. The process is often described as if it is some sort of replacement or alternative for offline radicalisation, Sageman draws a sharp distinction between the 'radicalized young men [that] were mobilized into terrorism by face-to-face interactions' (Sageman 2008a p.109) of the past from the then-modern form of radicalising on online fora. This seems to imply that to be radicalised online requires no interaction in the offline domain, or at least primacy in the online domain. This view is shared by other studies like the Anti-Defamation League (2014) as well as being one of the five hypotheses of the Von Behr et al (2013) study.

Other understandings take a notably different view. Bermingham et al. (2009) explicitly define the term as:

> A process whereby individuals, through their online interactions and exposure to various types of Internet content, come to view violence as a legitimate method of solving social and political conflicts (Bermingham et al. 2009, p.231)

In other words, they define the process by the effects drawn from online content, rather than being concerned with the domain in which an individual acted, either exclusively or primarily – this is seemingly shared in Neumann's (2013a) understanding of the term. In short, the majority of the time, no definition of the phrase is offered, and when there is, it can mean substantially different things.

To make matters more complicated, the phrase "self-radicalisation" is also often utilised in the literature. According to Macdonald and Whittaker (2019), who search for articles

relating to this term too, the phrase is both used in a conceptually ambiguous manner *and* it is sometimes used to mean a specific type of online radicalisation. They outline the differences in the term. Firstly, Von Behr et al. (2013) take the process to imply that a terrorist radicalises without any contact, physical or virtual, and the Institute for Strategic Dialogue (2011) for whom it merely precludes offline interactions. Meleagrou-Hitchens and Kaderbhai (2017) also note this discrepancy in the literature: 'For some authors, so-called 'self-radicalisation' (or radicalisation in isolation from wider networks) and radicalisation over the Internet are one and the same' (Meleagrou-Hitchens and Kaderbhai 2017, p.26). Self-radicalisation is, as Conway (2012) asserts, a fatally flawed concept because it overlooks the social process of radicalisation:

> One does not radicalise oneself in cyberspace, anymore than one is radicalised by oneself in the 'real world'... The concept of the violent online radical milieu thus works to show that ideas such as 'self- radicalisation' and 'self-recruitment' are effectively redundant. (Conway 2012, p.13)

In other words, the view that online interactions – both peer-to-peer or the consumption of propaganda – are not inherently social activities just because they take place online is an incorrect conceptualisation.

In Macdonald and Whittaker's (2019) study they highlight three reasons for the importance of conceptual clarity: undertaking robust research; communicating research findings to interested audiences; and conducting meta-reviews. The latter reason is important for the following chapter's literature review: if a concept has several common understandings and is not defined, then synthesising results may not be possible. In an ideal world, it may be preferable to aggregate the results of studies which analyse online radicalisation; it is often claimed that such systematic reviews are the top of the "pyramid" of academic inquiry (For example, see: Golden and Bass 2013). However, the lack of a common definition or even common understanding makes this impossible. The findings below offer several conceptualisations of what constitutes online radicalisation. As such, the literature review in Chapter 3 will review the concept as each author offers it, regardless of whether it refers to a cognitive or behavioural process or radicalisation, or however the researcher conceptualises the necessary interactions in the online domain. Where possible, these distinctions will be made and presented, however, the conceptual ambiguities outlined above, particularly the lack of definition in most cases, would make synthesising results in a systematic manner unattainable.

2.4 Understanding Radicalisation

2.4.1 Models and Theories

Several scholars have attempted to "model" the radicalisation process by offering different stages or factors that cause a person to engage in political violence. One of the best-known examples of this is Moghaddam's "Staircase to Terrorism" (2005), in which he conceptualises a five-step progression with fewer people ascending to each stage. The

ground floor contains millions of people with perceptions of injustice, of which only a small number move to the second level who experience anger and injustice and identify an enemy. On the third level, actors begin to engage with the morality of terrorist organisations and start to see such violence as a justifiable strategy, while the fourth level sees actors recruited to violent organisations and adopting an "us against them" outlook. The fifth and final floor involves training and participation in the actual terrorist incident (Moghaddam 2005). Rather than a model to be empirically tested, he suggests the staircase is a framework to organise psychological knowledge. This is, however, critiqued by Lygre et al. (2011) who challenge the linear nature of the model, suggesting that their literature review 'did not produce any empirical evidence supporting the prescribed order of psychological mechanisms… [which] question[s] the validity of Moghaddam's linear stepwise model' (Lygre et al. 2011, p.614). They also did not find empirical support for the psychological theories in steps three or four and question the value in excluding his model from empirical testing because the field of terrorism studies 'is in need of empirically and methodologically strong research' (Lygre et al. 2011, p.613).

Borum (2003) also offers a linear model as a psychological pathway to becoming a terrorist. He correctly observes that there is no universally applicable method to track every, or even most, trajectories, but instead claims that there are four observable stages that are common in the process. Firstly, he observes that individuals or groups tend to identify a problem or undesirable condition; this could be economic, social, or religious. Secondly, the problem is framed as an injustice compared to other groups, suggesting that the agent or group is being treated particularly unfairly. Thirdly, the diagnosed problem is attributed as being the fault of a target group, and finally, that target group is deemed morally responsible for the problem – he simplifies this as "it's not right", "it's not fair", "it's your fault", "you're evil" (Borum 2003). According to Borum, identifying a group as "evil" helps to facilitate violence, as it is more justifiable when it is aimed at bad people and it dehumanises the target group. He suggests that the model may help to identify agents who are at different stages of the trajectory. Similarly to Moghaddam's (2005) model, the empirical evidence of these stages were challenged, interestingly, by Borum himself years later, who admitted that the concepts were drawn from anecdotal and unsystematic analyses (Borum 2011b).

Several other models also offer a sequential understanding of radicalisation. Silber and Bhatt (2007) create a four-stage model of Islamist radicalisation: "Pre-radicalisation" describes an individual's life (their pedigree, lifestyle, religion, social status, neighbourhood and education) directly before their radicalisation process. Secondly, "Self-identification", in which individuals begin to explore Salafi Islam and base their identity around it. It is suggested that individuals most vulnerable to this are experiencing some kind of life crisis, which could include economic, social, political or personal factors. Next comes "Indoctrination", in which individuals fully adopt a jihadi-Salafi ideology while often withdrawing from their mosque and politicising their new beliefs. The final stage "Jihadization" includes the self-designation of the actor(s) as "holy warriors" and the operationalisation of this by way of an attack (Silber and Bhatt 2007). This is

relatively similar to the model offered by Precht (2007), who maps out four stages from "Pre-radicalisation" to "Action". Importantly, the model *is* sequential, but individuals do not follow a perfectly linear progression; allowing for individuals to engage in feedback loops and perhaps (although not explicitly stated) skip steps. The model heavily emphasises the role of ideology, claiming it to be 'the bedrock and catalyst for radicalization. It defines the conflict, guides movements, identifies the issues, drives recruitment, and is the basis for action' (Silber and Bhatt 2007, p.16). Given the critique of overplaying the role of ideology offered by Borum (2011c) and (Horgan 2008), it seems that this almost certainly understates other important factors. Silber and Bhatt (2007) also posit a lack of integration as a reason for radicalisation in Europe, a claim which has since been tested and rejected by several scholars (Vidino et al. 2017; Christmann 2012; Reynolds and Hafez 2017).

Helfstein (2012) posits a four-stage process consisting of: "awareness", "interest", "acceptance", and "implementation", but highlights that 'the nature of progression through these different stages is not uniform, and therefore the patterns and effects of social ties vary as people build their experience of radicalism' (Helfstein 2012, p.7). He notes that although some may follow the phase in a linear manner, others will rely on feedback loops from previous stages and some will skip steps. He also observes that the different stages have barriers to entry of ascending difficulty until one reaches acceptance, which facilitates easier implementation (Helfstein 2012). He argues that radicalisation cannot be fully understood as either an ideological or a social phenomenon, but instead as a process which integrates the two. Stressing the importance of social networks is important, few would argue against this point, but much of the literature, including the three models identified above (Borum 2003; Moghaddam 2005; Silber and Bhatt 2007) frame the process primarily as a personal one, potentially overlooking the importance of social interactions.

Despite models like the ones above being posited within the literature, there is little explained reason, for the most part, to believe that those radicalising actually go through a linear process. Borum (2011b) notes that despite these types of models becoming popular with law enforcement, the accuracy and stability of these models has not been tested. Similarly, in their review of five conceptual models, including three offered above, King and Taylor (2011) argue that multi-stage models are practically impossible to test empirically because confirming that each individual goes through the requisite stages is too-high of an evidentiary bar. They suggest that the best that can be hoped for is to test stages individually. One might therefore question the benefit of these models. Both Borum (2003) and Moghaddam (2005) claim that their models are not meant to be empirically tested, but rather as heuristics for social science theories, but given the objections to the evidence-base of these theories, as outlined above, this seems dubious. Recently, there has been some work developing the model created by Silber and Bhatt (2007) into a "dynamic risk assessment" of radicalisation trajectories (Klausen et al. 2016; Klausen 2016a; Klausen et al. 2018), although they admit they have to modify the original model by downplaying the role of ideology, which Silber and Bhatt (2007) claim

drive the process (Klausen et al. 2016). However, their focus specifically on sequencing behaviours related to four discrete stages suggests that Silber and Bhatt's model may have some value as an empirical basis.

Rather than trying to plot a multi-stage process, other scholars have taken a different approach, offering factors that are present in the process. McCauley and Moskalenko (2008) offer twelve mechanisms which tend to be present within the radicalisation process,[3] offering several different theories from social science to support each mechanism, although they do not propose an underlying theory uniting all twelve together. Individually, none of the mechanisms can explain how the process works:

> It is unlikely that any one of these mechanisms is sufficient to explain political radicalization…The list of twelve mechanisms are neither sufficient causes one by one nor instantiations of some larger theory. Rather, we suggest that there are multiple and diverse pathways leading individuals and groups to radicalization and terrorism. (McCauley and Moskalenko 2008, p.429)

It is also important to note that only two of the twelve mechanisms occur at the personal level, while the rest require a degree of social interaction. More recently, they have updated their model to separate between different processes of radicalisation towards violence and cognitive radicalisation (McCauley and Moskalenko 2017). They acknowledge the importance of the distinction between the two, as argued by Horgan (2008) and Borum (2011c) above, and conclude that 'There is no "conveyor belt" from extreme beliefs to extreme action. It is plausible that radical beliefs inspire radical action, but research has indicated that the connection is weak' (McCauley and Moskalenko 2017, p.213).

A similar strategy is taken by Webber and Kruglanski (2017) who offer a psychological "3 N's" model of radicalisation. They build on the theory that those that radicalise all share a "quest for significance", which Kruglanksi and others have posited elsewhere (For example, see: Dugas and Kruglanski 2014; Kruglanski et al. 2014; Jasko, LaFree and Kruglanski, 2017; Webber et al. 2018). Their model suggests that all radicalising individuals have "needs" of two types: individual and social. All the motivations that pertain from this – such as honour, humiliation, injustice, vengeance, and social status – can be conceived as part of a quest for significance (Webber and Kruglanski 2017). They also highlight the importance of "narratives", in other words ideology; one must identify a grievance and an out-group. Furthermore, these narratives often present the notion of opting to engage in violence for the cause as a means to gain significance. Finally, individuals enter into "networks" in which they find a second family and begin to intertwine personal views with the groups' collective views. As with McCauley and

[3] 1) Perceived personal victimisation, 2) Political grievance, 3) Joining a radical group (the slippery slope), 4) Joining a radical group (the power of love), 5) Extremity shift in like-minded groups, 6) Extreme cohesion under isolation and threat, 7) Competition for same base of support, 8) Competition with state power, 9) Within-group competition, 10) Jujitsu Politics, 11) Hate, 12) Martrydom.

Moskalenko (2008), there is no requirement for a specific sequence of these factors, nor do they insist that each must necessarily be present.

Bouhana (2019) also offers a non-linear model as a framework for radicalisation. Drawing from Situational Action Theory, which seeks to understand the interactions between people and their environment and how the latter may encourage involvement in crime (Wikström and Bouhana 2017). Bouhana's (2019) model includes with individual susceptibility – i.e. what characteristics an individual that may predispose them to becoming radicalised. This can be exacerbated by the individual's exposure to certain people, locations, or ideas; she demarcates "social selection," such as residence and socioeconomic status, from "self-selection," where individuals choose to spend their time. This is in turn affected by the different affordances that the settings offer individuals, such as whether certain settings encourage extremism or whether they fail to discourage social or legal norms. One level up from these settings is the social ecology – the communities that may support the emergence or maintenance of these affordances. Finally, the model includes the system-level factors, such as social norms, governance, and strains. These system level factors play a role in the emergence of social ecologies but also affect the susceptibility of individuals.

There have also been several theoretical contributions to explain the process of radicalisation. For example, Borum (2014) lists several unfulfilled needs that can lead to a "psychological climate" for radicalisation including pro-violent attitudes, grievances, sensation seeking, and disinhibition. Sageman (2004) posits the role of brotherhood and kinship as important in his "bunch of guys" theory, while Veldhuis and Staun (2009) emphasise the importance of frustration. Furthermore, in his literature review on the topic, Borum (2011a) lists a number of theories which have been posited as lenses to view the radicalisation process, including: Social movement theory, groupthink, in versus out-group dynamics, extremity shifts, and conversion theory. The role of stress has also been highlighted as a potential factor (Canetti et al. 2013), as have uncertainty (Hogg et al. 2013; Hogg and Adelman 2013; Pruyt and Kwakkel 2014), the quest for significance (Dugas and Kruglanski 2014; Kruglanski et al. 2014; Jasko, LaFree and Kruglanski 2017; Webber et al. 2018), and mortality salience (Pyszczynski et al. 2006).

2.4.2 A Complex Phenomenon

The non-linear models outlined above underlie the complexity of the radicalisation process. Rather than trying to identify discrete stages which actors go through, they posit factors which may be present. This seems like a fuller understanding of the process. Borum (2017) notes that the most striking feature of radicalisation is its diversity from case-to-case and trying to accurately discern and model it may not be a fruitful exercise, particularly given that we still know so little:

> While much about radicalization remains empirically unvalidated, it is clear that the process is multi-determined, and that its etiology often includes broad grievances that "push" an individual toward a radical ideology and the narrower,

> more specific "pull" factors that attract them. Many times, the factors are transactive (affecting each other). (Borum 2017, p.28)

Other scholars have also argued that the process is too complex to substantiate in a simple model or theory (Silva 2018; Guhl 2018; Hafez and Mullins 2015). Jensen, Atwell Seate and James (2018) note that research on radicalisation has been ontologically and methodologically flawed:

> Research on extremism continues to treat the phenomenon as one that can be understood through the development of simple linear process models or through the identification of small sets of cognitive, emotional, and behavioral traits that are believed to be common to extremists. Research shows that these models struggle to account for the radicalization trajectories of many extremists while also contributing to the proliferation of misleading radicalization profiles (Jensen, Atwell Seate and James 2018, p.2).

That is to say, they miss a number of true negatives of those that engage in violence but do not 'radicalize" in any traditional sense' (Borum 2011c, p.2). Conversely, they also do not seem adept at explaining false positives; individuals that go through all the stages (or fulfil the criteria) but do not engage in violent behaviours.

Similarly, despite the range of theoretical contributions to the field, there remain more questions than answers. Few have been empirically tested and even fewer have been tested rigorously to support the hypothesis of engagement in violence. Jensen, Atwell Seate, and James (2018) note that:

> Radicalization research has not focused on the rigorous empirical testing of key theoretical propositions, making it difficult to judge how well the theories work as general explanations of radicalization processes. Instead, most theories are supported by limited case evidence and many researchers do not reference case selection criteria or the logic of inference that is being employed in their studies. (Jensen, Atwell Seate, and James 2018, p.2)

In his review of theories to explain radicalisation, Borum (2011a) notes that: 'None of the theories discussed here provides easy answers. No single theory is likely to explain all violent radicalizations' (Borum 2011a, p.31). Given the lack of consensus both at the empirical and theoretical level, it is unsurprising that scholars have started to assess factors from a "multifinality" perspective (Corner, Bouhana and Gill 2018)

2.4.3 Empirical Radicalisation Research – What we know

This is not to say that there are no insights into the dynamics or processes of radicalisation, merely that there are not presently theories which can explain a cause-and-effect process. Typically, studies have tended to demonstrate that there is a lack of commonality between radicalised individuals. Vidino, Marone and Entenmann (2017) note that their sample of terrorist attackers is heterogeneous demographically, while

Bakker (2006) notes that his sample has more dissimilarities than similarities. Silber and Bhatt (2007) note that there is no useful profile that can be used, which Horgan (2008) agrees with, noting that attempts at creating a terrorist profile have repeatedly failed. Corner, Bouhana and Gill (2018) note that in the literature the following factors and indicators have been associated with radicalisation: poor integration, poverty, relative deprivation, the Internet, social interactions, prisons, mental disorders, and personality characteristics. Gill (2016) notes that the large number of variables that posit a relationship with radicalisation is problematic for future research because they lack weighting and indicators are not all equal; he argues that this has led to 'the radicalisation literature lack[ing] specificity in terms of what it is studying the indicators of' (Gill 2016, p.7).

Despite there being no suitable terrorist profile, research has suggested some general demographic trends. Several database studies have found that over 95% are male (Horgan et al. 2016; Bakker 2006; Sageman 2004; Gill et al. 2015; Vidino, Marone, and Entenmann 2017), although research into ISIS foreign fighters has been slightly more even, with around 80-85% being male (Cook and Vale 2019; Reynolds and Hafez 2017). Moreover, terrorists tend to be young. In their study on UK terrorists, Gill et al. (2017) find a median age of 27; a mean of 28; and a mode of 22, although this exists between a range of 16-58. Other studies have come to similar conclusions: Both Sageman's (2004) Reynolds and Hafez's (2017) respective samples have a mean age of around 26, while Bakker's (2006) and Vidino, Marone, and Entenmann's (2017) are 27.

Socioeconomic factors are often posited as a potential cause or stressor in radicalisation, although there is little consensus within the academic literature. Sageman (2004) found that in his terrorism database, underemployment played an important role, but Bakker's (2006) sample challenges this, finding there to be no typical similarities within samples. Other database studies have found between a third (Gill et al. 2015) and 12% (Horgan et al. 2016) to be unemployed. In their sample of German foreign fighters, Reynolds and Hafez (2017) find socioeconomic integration to be a poor predictor of individuals choosing to travel, while LaFree et al. (2018) find that around 70% of their US based sample of terrorists to have a stable employment history. At the macro level, Piazza (2006) finds that poorer countries *do not* produce more international terrorists, but does find that minority economic discrimination is a strong predictor of domestic terrorism (Piazza 2011). Cruz and colleagues (2013) find that labour force participation (i.e. the active workforce) is negatively correlated with the frequency with which a country experiences acts of terrorism. There is a longstanding academic study of these factors, which Schmid summarises as: 'The fact is that empirical research has not been able to establish a direct link between collective or individual poverty and terrorism. In other words, this is a myth or at best a half-truth' (Schmid 2013, p.25). He does, however, suggest that this may not hold over all countries and that certain economic measurements, such as underemployment may play a role.

The role of education in radicalisation has also been contested in the academic literature. In some empirical research, terrorist samples have been found to be relatively well educated, with the large majorities having completed secondary education (Bakker 2006; Sageman 2004), and sizable minorities having tertiary qualifications (Horgan et al. 2016; Gill et al. 2015; Bakker 2006; Sageman 2004). In some instances, terrorist populations have been found to demonstrate a higher level of education than the general population from which they come (Berrebi 2007). In their study of US-based terrorists, LaFree et al. (2018) test the hypothesis that an increase in educational attainment will decrease the probability of engaging violence. Bivariate analysis which compares extremists that commit violence against those that do not supports this hypothesis, although conducting a multivariate analysis, they find that it had no significant predictive effect when controlling for other behaviours.

Research has pointed towards a clustering of radical individuals or networks, which experience larger mobilisation or recruitment than one may otherwise expect. These are sometimes called radicalisation "hotspots" or "hotbeds." In their study of IS terrorists in the West, Vidino et al. (2017) note that actors are distributed unevenly, even if accounting for factors such as integration. They posit that a concentration of a small number of charismatic leaders play a key role in a bottom-up network of peers. This point is also made in relation to foreign fighters by the Soufan Group (2015), who suggest that this is a key determinant to mobilisation to Iraq and Syria. Several hotspots have been identified in the academic literature such as Molenbeek in Belgium (Van Vlierden 2016) Derna and Sirte in Libya (Varvelli 2016) and Minneapolis/St Paul in the US (Vidino, Harrison, and Spada 2016). In their sample of 99 German foreign fighters, Reynolds and Hafez (2017) find support for the hypothesis that such clustered networks were the most important factor in mobilisation. This is in line with the theoretical arguments of Bouhana (2019), who notes that extremism-enabling settings are not equally distributed in space and time; some environments contain specific contexts which encourage – or fail to suppress – extremist behaviours.

Another factor is the potential over-representation of converts in jihadist terrorism. Several scholars have observed that there appear to be many more within contemporary cohorts than in previous decades (Klausen 2016b; Sedgwick 2010). Azani and Koblentz-Stenzler (2019) find that European Muslim converts are over-represented in radical jihadism. Taking the United Kingdom as an example, they observe that converts make up less than 4% of the Muslim population, but constitute 12% of the radiacl jihadist population. Fodeman et al. (2020) empirically test if this may be the case by surveying 356 American Muslims, half of whom are converts, and comapre the two groups. They find that the convert group exhibits higher activism and radicalism than the control group suggesting that they may be more likely to engage in violent behaviour such as terrorism. Halverson and Way (2012) argue that it is related to the "mystique" of Islam offering disaffected and criminally predisposed individuals a new start in life, while Hafez and Mullins (2015) state the promise of an afterlife is attractive to individuals who have a

background in crime, and these individuals may be knowledge-hungry and restless when presented with a new meaning in life.

Radicalisation research has also focused on the previous criminal experiences of terrorists. Basra and Neumann (2016) describe the dynamics of what they call the "crime-terror nexus" by drawing from a database of 79 European jihadists. They find that criminal and terrorist groups often recruit from the same population and that the personal needs and desires of criminals are similar to those of terrorists. Overall, they find that 57% of their database had been previously incarcerated, often for petty or violent crimes rather than ideologically motivated ones. The database studies of Horgan et al. (2016) and Vidino et al. (2017), have similar results, finding that 61% and 57% of their respective samples had criminal histories. The number is slightly lower in the research of Sageman (2004) and Bakker (2006) found that roughly a quarter of their respective samples had criminal records, but that those without a record had often been involved in activities without apprehension. Noting that criminologists regard having a criminal record as being one of the best predictors of future criminal behaviour, LaFree and colleagues (2018) hypothesise that individuals with a record will be more likely to engage in violent extremism, for which they find support, regardless of whether the previous activity was violent or not. Their finding also holds in multivariate analyses when controlling for other factors. Conducting a meta-review of risk indicators of radicalisation, Desmarais et al. (2017) find that find there to be some support for the relationship between previous criminal activity and engaging in terrorism, but note that offending ranges varied substantially, but problematically, studies rarely employ a control group.

The role of mental health disorders and involvement in terrorism has been hotly debated in academic scholarship for several decades. Gill and Corner (2017) observe four paradigms in this research, the first suggesting psychopathy was a cause of terrorist involvement, the second focused on personality types, the third synthesised the previous evidence and critiqued the body of knowledge, while the fourth, focused on empiricism outlines the range of pathways and different push and pull factors that may reinforce radicalisation. Scholars have often noted that terrorists do not suffer abnormal levels of mental health issues (Horgan 2008; Borum 2014; Venhaus 2010; Webber and Kruglanski 2018), although with the caveat that lone actor terrorists may have a higher disposition to specific disorders (Corner, Gill and Mason 2016). LaFree et al. (2017) hypothesise and find evidence that actors that display mental illness predicts engaging in political violence. Vidino and colleagues note that their cohort of terrorists, 'metal issues appear to have played a role in the actions of perpetrators of attacks' (Vidino et al., p.69). Neither of these studies disaggregated into specific disorders. Conducting a review of the empirical literature on psychopathology and terrorism, Corner and Gill (2018) outline a number of studies which do find a relationship between disorders and involvement in terrorism, but note caution against assuming causality – active symptoms may be present, but unrelated to engaging in violence.

2.5 Conclusion

One cannot undertake research into online radicalisation without first examining the word "radicalisation". Within the academic literature, it is definitionally unclear, referring to a process of one of three non-causally related phenomena: terrorism, extremism, and radicalism. At the heart of this ambiguity is a disagreement over whether the process is cognitive (i.e. leading to the adoption of a set of radical or extreme beliefs) or behavioural – i.e. leading to the adoption of a set of (sometimes violent) behaviours, often including the adoption of beliefs along the way. Moreover, each of the stem words have normative connotations which add further inconsistencies. Terrorism and extremism are deemed to be normatively bad, but are contested because policymakers have "defining agency" to use the words politically. Radicalism, on the other hand, can range anywhere from synonymy with the word terrorism, to a normatively good quality in which someone attempts to change the world for the better. This, too, can add to the ambiguity of the word. This ambiguity compounds with other factors to cloud what is meant by "online radicalisation," leaving both scholars and interested audiences unclear as to what the process entails.

This conceptual ambiguity has negatively impacted our understanding of how the process actually works. Various attempts have been made to conceptually model or theorise the process, either by positing a multi-stage trajectory or by highlighting mechanisms that take place. However, these tend to exist only at a theoretical stage, with little scope for empirical testing. There is a growing empirical literature on the different factors that are present in radicalised individuals, and although no common pathway exists, some characteristics or life experiences are more prevalent than others. Although there are dozens of risk factors and vulnerabilities, none are necessary or sufficient.

Chapter 3: Online Radicalisation Research

3.1 Introduction

This chapter reviews the existing literature on the phenomenon of online radicalisation. To begin, it will survey the attempts that have been made to theorise the concept, drawing from scholars that have mapped out potential dynamics as well as models of the process. Given that these theories often posit a sharp online/offline dichotomy, the chapter will then discuss an ontological viewpoint which challenges this notion, instead arguing that the two domains are not separable in any meaningful way. Following this, the existing empirical research will be discussed, having been divided into two categories. Firstly, the "demand-side" of online radicalisation, which seeks to understand how individuals have used the Internet as part of the trajectory towards terrorism or extremism. Secondly, the "supply" of radical IS content available to would-be terrorists on the Internet such as propaganda and activity on social media.

Several inferences are drawn from this: Firstly, existing theories and models have not yet adequately explained how using the Internet affects radicalisation. Many of the points are imported from other aspects of social science and have not been tested rigorously. The theories also tend to assume a relationship between engaging with radical content and becoming radicalised, which is not yet proven – although some theorists are equivocal about this relationship. Moreover, most theories tend to assume a problematic ontological dichotomy between acting online and offline. Secondly, the nascent, yet growing field of the demand-side of online radicalisation research suggests that the Internet is central in contemporary terrorism plots. However, research tends to suggest that this does not come at the expense of offline interactions – therefore online radicalisation *has not* replaced offline radicalisation. Thirdly, research into IS online demonstrates that they had a sophisticated and wide reach up until around 2016, at which point it experienced a notable decline, causing supporters of the group to become more adept in the face of a hostile online ecosystem. The supply of content also reveals important insights into the role of gender in the online space as well as the significance of low-level content such as memes and video game motifs. The chapter concludes by synthesising the literature, identifying gaps and formulating the research questions which will dictate the quantitative enquiry of Chapter 5:

RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?

RQ2: Has the online domain replaced the offline one as the primary venue for terrorists' antecedent behaviours?

RQ3: Do terrorists that act online demonstrate different experiences to those that do not?

RQ4: Does acting on the Internet help or hinder terrorists?

3.2 Theorising Online Radicalisation

Despite the conceptual and definitional ambiguity surrounding the phenomenon, several scholars have attempted to theorise how the Internet may facilitate the process of radicalisation. This section will first review the existing theories and dynamics which have been proposed, before moving on to the models of online radicalisation which seek to offer pathways of factors which build upon each other. Finally, given that these theories and models tend to posit a distinct ontological dichotomy between the online and offline domain, this section will introduce philosophical positions which challenge this distinction and argue that it is not fit for purpose.

3.2.1 Theories and Dynamics

Neumann offers six processes and dynamics drawn from the literature which help to explain 'how online radicalization works' (Neumann 2013a, p. 435). The first two relate to exposure to extremist content: Pyszczynski *et al.* (2006) argue that watching suicide operations and beheading videos can lead toward *mortality salience* which leads individuals to consider their own mortality and increases support for violence. He also highlights Sageman's (2008) argument that viewing videos from conflict zones in which Muslims are suffering at the hands of Western troops creates a *sense of moral outrage* which can act as a trigger for mobilisation for violence. Neumann is careful to note that 'no single item of extremist propaganda is guaranteed to transform people into terrorists' (Neumann 2013a, p. 435) but that online radicalisation results in individuals being immersed for prolonged periods of time. This claim is more assertive than Conway (2016a), who argues that there is no proven connection between the consumption of extremist content and engaging in violent extremism.

The third and fourth mechanisms relate to online communities: Neumann (2013a) argues that the Internet can act as a *criminogenic environment* in which deviant behaviours are learned and normalised (Sutherland 1947). Neumann links this to the idea of an online echo chamber in which like-minded people congregate, pushing moderating voices out, which in turn skews individuals' perceptions of reality towards the voices that advocate violence. The idea that homogenous groups can lead towards unwanted outcomes is well-trodden ground in social science; Janis (1971) coined the idea of "groupthink" half a century ago in which individuals seek concurrence to the point to the point of overriding alternative courses of action, while Sunstein (2002) argued that "group polarisation" tends to push sentiment towards the most extreme views of their members. However, despite being hypothesised as playing a role in pathways towards terrorism, there is little empirical evidence to suggest that this is the case (O'Hara and Stevens 2015; Whittaker 2020). Neumann suggests that these criminogenic environments are exacerbated by online communications being more hostile due to due the lack of face-to-face communication between participants – known as the *online disinhibition* effect (Suler 2004). The anonymity, asynchronicity, and dissociative imagination that the Internet provides act out with more intensity that they would offline.

The fifth process relates to the interplay between the social and interactive nature of the Internet. Neumann (2013a) suggests that individuals *role-play* an idealised version of themselves online. This avatar will often by more zealous and supportive of violence. He draws on the theoretical argument of Brachman and Levine (2011) who suggest that the constant role-playing eventually becomes depressing because individuals observe the discrepancy between their idealised roles and their "real" lives. From this point, a small number will choose to bridge this gap by moving towards their idealised avatar. The final dynamic is simpler; it relates to the Internet's ability to connect individuals with similar interests across great distances and no previous interactions. While previous generations' jihadists may have met and communicated in radical mosques, the Internet offers a far larger recruitment pool that can be tapped into with less risk (Neumann 2013a).

Sageman (2008) argues that argues that there several differences between the Internet and offline interactions which can have dramatic effects on radicalisation: Firstly, he notes that the semi-anonymity of the Internet is leading to the gender separation of jihadist movements to disappear. Secondly, the average age plummeted as a new generation of Internet-savvy young adults joined (Sageman 2008a). Thirdly, people express more vitriolic views online, potentially – although not explicitly – referring to Suler's online disinhibition effect (Suler 2004). Fourthly, when people disagree with radical views online, there are easier exit ramps for them – they can just log off – leaving the most radical views to fester. Fifthly, they have a non-hierarchical structure – he argues that even if Osama bin Laden were on a forum, he would not be able to exert the same authority and control that he would offline. Finally, he argues that unlike on-the-ground movements, there is little incentive for online radical communities to evolve beyond terrorism (Sageman 2008a).

Ducol et al. (2016) conduct a review of the academic literature into social psychology of the Internet to hypothesise potential dynamics of violent extremism. They posit several factors that may be different online that could exacerbate radicalisation. They note that although individuals identify as part of social groups in both domains, the Internet may provide an opportunity for individuals to participate in new groups and the anonymity may trigger a process of deindividuation – aligning behaviours with that of the group and creating a diffusion of responsibility (Spears et al. 2002). They also argue that online activity may amplify attraction towards a specific in group while increasing negative views towards an out-group, triggered by anonymity and deindividuation which may trigger a perceived threat to an individual's own identity (Harris et al. 2014). Ducol and colleagues (2016) also argue that selective exposure may create a cognitive bias which promotes polarisation of opinion – they link this to both self-selected (i.e. echo chambers) and system-selected (i.e. filter bubbles) exposure. The Internet may also act as an outlet for individuals to express their "true self", sharing their stigmatised identities with an easily discoverable group of like-minded people online (Slater 2002; McKenna and Bargh 1998).

As well as attempting to understand these key areas of research, Ducol and colleagues (2016) also draw on the social psychology of online interpersonal relationships to attempt to understand radicalisation. They draw from Social Information Processing (SIP) Theory, who attempts to explain how people manage relationships online, without the verbal cues that are available in face-to-face interactions. Although SIP posits that relationships take longer to build online, they may eventually result in more intimacy and connection than offline (Walther 1996). They also suggest that individuals tend to seek out homophily, for which social media platforms are specifically designed, encouraging users to "follow" or "friend" others. This may create an environment in which deviant subcultures are more easily formed. These types of deviant subcultures are aided by the secrecy and anonymity that is provided by the Internet, as well as providing settings which are prone to collective dynamics by leading to more agreement towards in-group influence (Ducol et al. 2016). However, they note that the literature on the psychology of the Internet is a small and growing field, and the dynamics outlined above are merely factors that *could* affect radicalisation. Moreover, like Neumann (2013a), they play down the idea that mere exposure to radical content promotes radicalisation, but instead posit that it is conditioned by the environment in which it is received. They also note that the Internet is only one variable among dozens that are associated with radicalisation.

Koehler also advances a theoretical explanation to understanding online radicalisation. He conceptualises radicalisation as a process of depluralisation from political concepts and values (such as justice, freedom, and democracy according with the concepts of a specific ideology. The more that individuals believe there is no alternative to their ideology, the higher degree of radicalisation (Koehler 2014). Koehler argues that the Internet is a main facilitator of this process as it provides an ideological pillar with the infrastructure of a radical social movement. It provides a cheap and efficient communication where individuals can share crucial information as well as a constraint-free space with anonymity in which individuals can become "more" than their offline personas. It also gives a perception of a larger critical mass of the movement than actually pertains and an opportunity for individuals to directly reflect on the effects on propaganda. Koehler argues that the Internet is the most important space to learn the necessary skills to join offline groups and advance within the social hierarchies and therefore is a major driving factor to establish and foster the development of what he calls "radical contrast societies" which transmit violent ideologies and transmit them into political activism (Koehler 2014).

Docul (2015) critiques many of the theoretical discussions surrounding online radicalisation. He notes that arguments in favour of the Internet having a significant role in radicalisation seem to be based on the problematic premise of a causal link between the availability of extremist content and anecdotal cases of individuals engaging in terrorism – which he likens to the new discredited "magic bullet" (or hypodermic needle) model of communications. He also argues that the dichotomy of "virtual" vs "real" is problematic as it implies two autonomous spaces that do not affect each other. Docul argues that theory has typically asked the wrong question – "instead of asking "what does

the Internet do to people? We should…reverse the question and consider "what do people do with the Internet?"" (Ducol 2015, p. 89).

Ducol suggests that Situational Action Theory (SAT) – the intersection between cognitive schemes and social settings and how they affect engagement in crime – can be used to better understand radicalisation (Ducol 2015). He argues that daily life is composed of several "life-spheres" which can be online or offline (for example: friends, family, social media, websites); if enough of an individual's life-spheres become interlocked, the more it will affect their socialisation settings. Ducol notes that online and offline life spheres have their own characteristics borne out by the affordances the Internet provides and can be either largely independent or strongly intertwined. However, a radical sociability may lead to a gradual cognitive monopoly which in turn will lead to a progressive crystallisation of beliefs and identity in both domains. Essentially, the Internet alone does not radicalise people, but represents one of multiple environments that cannot be fully understood without close examination into the relational settings interactions them (Ducol 2015).

3.2.2 Online Radicalisation Models

Several scholars have attempted to model the process of online radicalisation. Saifudeen (2014) suggests that the Internet is often relegated to the role of being a mere facilitator in the process of radicalisation which overlooks the unique attributes and community dynamics of the Internet realm that contribute to the radicalisation process. He suggests that several dynamics are fundamentally different online, such as it being a safe haven for deviant counter-culture; that it is akin to a buyers' market in which individuals can pick and choose information and communities at their will; and the competing pulls that exist from the range and diversity of narratives and options which push individuals in pathways which are fluid, unstructured, and multidirectional (Saifudeen 2014). He also draws upon research which suggests that information on the Internet is "sticky" and bite-sized which makes it easily digestible for a Web 2.0 audience and exploits human's heuristic-based processing of information.

Saifudeen (2014) uses an analogy of planetary orbits to model online radicalisation (Figure 2), offering five levels: Scepticism, Validation, Activism, Extremism, Violent Extremism. The individual remains in the orbit of their chosen online counter-culture which reinforces their current mindset. At the same time, there are a range of competing "Gravity Wells" which can pull an individual further inward towards the next level. However, given the competing information in cyberspace, the orbit can be transitory and if the orbit is not able to remain credible then an individual can fall back out. This culminates with an individual beginning to take absolutist worldviews, linear non-critical thinking and advocating violent solutions, which Saifudeen argues is very difficult to return from. This orbit continues until events or opportunities arise for the individual to conduct acts of violence, and therefore entering the centre stage of the model. He also notes that online dynamics can cause individuals jump orbits very quickly given the speed of information absorption and resonance in cyberspace. The benefit of the orbit

approach, according to Saifudeen, is that they represent a range of different pathways as opposed to linear progressions; an individual only stays at one level for as long as gratifications and motivations remain effective, which explains why some individuals remain at one level without progressing (for example nonviolent extremists).

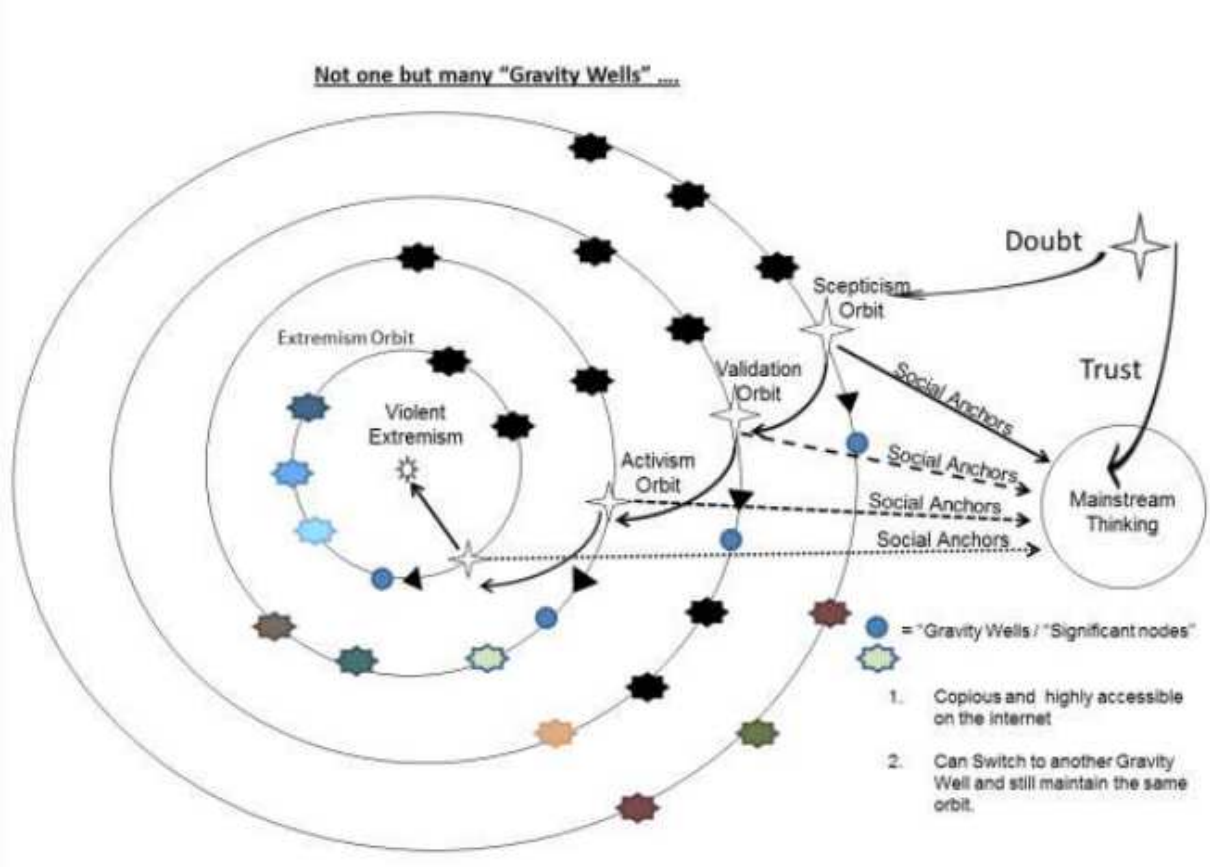


Figure 2 - Saifudeen's (2014) Cyber Orbit Pathway Model

Bastug, Douai and Akca (2018) propose a four-step model of online radicalisation based on the empirical findings of their work on jihadist foreign fighters from Canada (Figure 3). The first step is the *Accessibility and Proliferation* of online content, for example via Twitter or online jihadist magazines. The second step relates to the *Susceptibility and Pre-Disposition* – the social and psychological factors which explain why extremist messages resonate with a select audience. This moves to the third step of *Terrorist Mobilization*; they argue that social media plays an active role in the recruitment process, discussing the charismatic sermons of Anwar al-Awlaki which has traces into several plots in their sample. The final step is where individuals who have been mobilised *Share* their own experiences and messages online, which creates a feedback loop of new content that is available for potential recruits. Bastug, Douai, and Akca (2018) note that the model explains how online radicalisation occurs, but little is explained as to whether the Internet plays a causative role. Rather, it seems to be an explanation of how recruitment can occur on the Internet, rather than an individual-level model. Moreover, their model implies a sequential process between engaging with terrorist content and mobilising

towards a terrorist group, which is an assumption that has been criticised in the academic literature (Sageman 2014; Archetti 2015; Aly 2017; Conway 2016a).

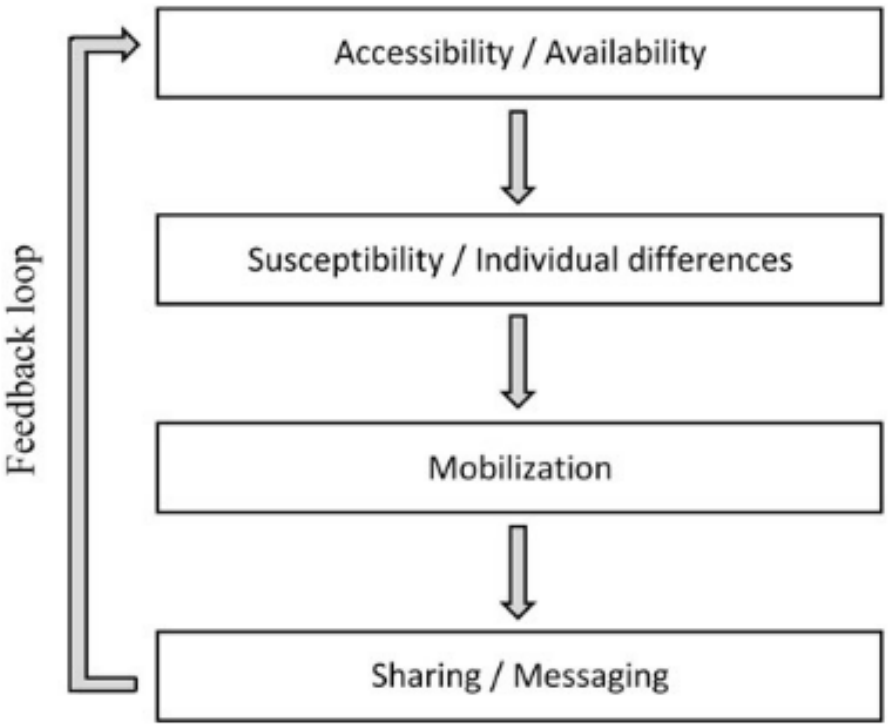


Figure 3 - Batug, Douai, & Acka's (2018) Four Step Model of Online Radicalisation

Neo (2016) posits a five-stage online radicalisation model which seeks to account for the interactions between humans and systems that occur in a complex online environment (Figure 4). The first stage *Reflection* which refers to propensities and vulnerabilities that an individual may have, as well as the personal or social factors that may cause individuals to open-up to new information. This leads many individuals in this phase turn to the Internet for solutions. Like Saifudeen (2014), Neo argues that the wide array of ideas available offer many opportunities for cognitive openings to occur and an individual's worldview can be challenged. Moreover, the Internet's anonymity facilitates an environment where an individual can experiment with an array of ideas with little consequence. This is followed by *Exploration*, in which an individual begins their search for alternative belief systems. Their receptivity to these will depend on the propensities of the previous step, meaning that the first two phases occur in parallel. Neo notes the importance of the Internet as a visual medium in this phase, as well as the speed, depth, and volume of information that can be accessed. These online exposures can help to frame and prime individuals to a new potential worldview and that the radical narratives that can be found are famed in a way that will resonate with their target audience. This too falls victim to the unproven connection between radical content and engaging in violent extremism (Conway 2016a).

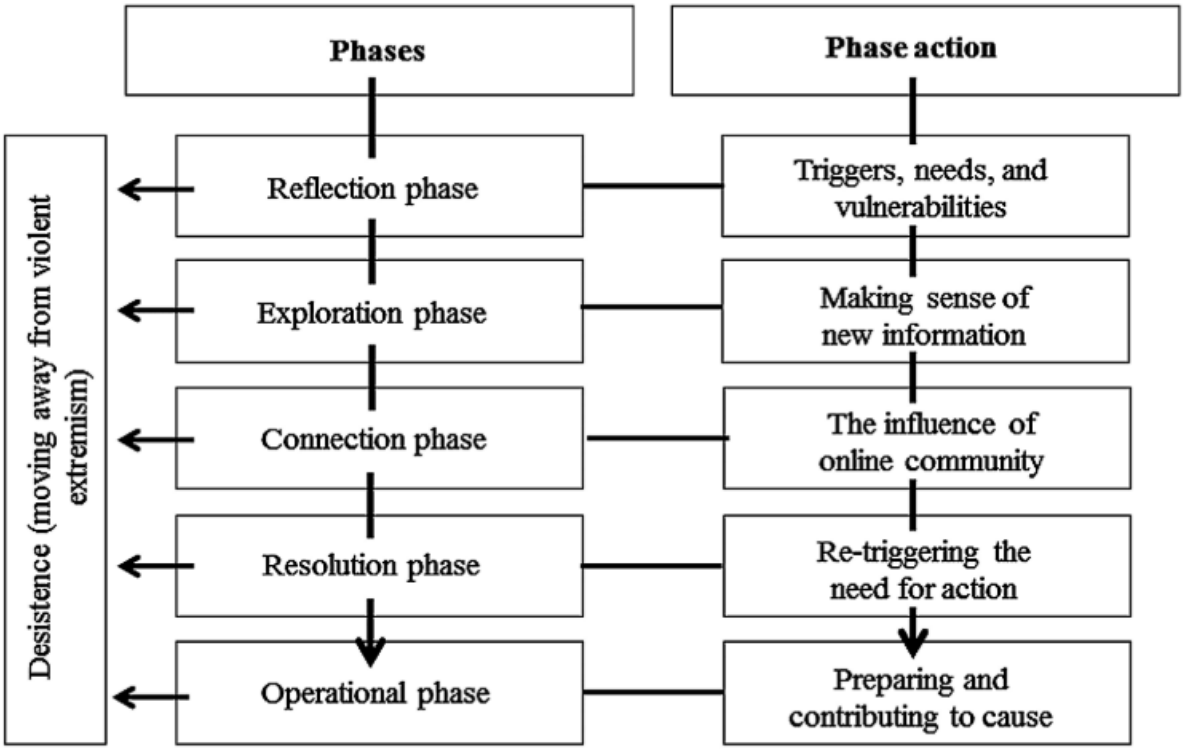


Figure 4 - Neo's (2016) RECRO Model

If an individual finds gratification within those parallel steps, then they may interact with like-minded people in the *Connection* phase. Like Neumann (2013a), Neo emphasises the potential of homogeneous ideas that normalise extreme viewpoints – an online echo chamber effect. These online communities also facilitate new rules of social conduct and behaviours, which can encourage moral disengagement. Neo also points to the interactive nature of the Internet which creates a shared online community that can overcome an individual's offline environment. From this point, an individual can enter the *Resolution* phase in which radical beliefs can gain traction into action. He notes that most individuals with such ideas do not act upon them. However, the Internet may provide an environment in which individuals attempt to become the prototype of an ideal member that they have consumed in propaganda. This is followed by the *Operational* phase in which an individual is mentally and/or operationally prepared to play a role in a plot. A key part of this is gaining access to the necessary individuals and resources, which Neo notes may require access to "real world" networks. That being said, the Internet can still be used to learn new skills and influence others (Neo 2016).

Torok (2013) offers a post-structuralist model to explain online radicalisation which posits that the Internet is akin to a Foucauldian institution in which networked power operates to recruit and radicalise. She argues that there are several dynamics which help to achieve this, such as the online environment acting as an isolating influence; it being a powerful tool to influence thoughts and behaviours; and a flatter and more distributed power structure than offline networks. She likens the online environment to Foucault's

"Castles" which, like a physical castle, is a self-imposed form of self-isolation and training that individuals enter willingly which breeds ideological homophily. Within these online castles radical beliefs and behaviour are normalised (perhaps an implicit reference to an online echo chamber). Moreover, a key dynamic within online environments is the polarisation of these beliefs in which individuals categorise themselves as part of an in-group and denigrate a targeted out-group. Social media is also ideally placed as an important forum in which discuss issues with emotional triggers. Torok's (2013) model does not appear to be linear but rather seems to be a description of several potential dynamics which appear to prescient on the Internet as opposed to offline institutions.

Weimann and Von Knop (2008) propose a five-stage radicalisation process which they apply to the online environment. This begins with the *Searching* phase in which individuals looks specifically for information to fulfil their personal or spiritual needs, followed by the *Seduction* phase where they are introduced to radical ideologies via online websites. Then, users enter the *Captivation* phase, which 'is the most important one because in this phase the users start to visit blogs, forums, and chat rooms and become attracted by their seductive messages' (Weimann and Von Knop 2008, p. 890). Then then follows an integration with the online community where users enter the *Persuasion* phase. They note that for most, the road ends here, but a select few enter the *Operative* phase where they gain access to operational contacts and materials online and may be invited to join a terrorist organisation. They note that during the online radicalisation process, the individual is still interacting with the outside world (e.g. friends/family/mass media), so they are therefore not totally isolated. They note several dynamics which explain how this process works, including the anonymity of the Internet; the fact that websites cater to alienated members of Muslim diaspora communities; and the acceptance and approval that individuals gain when entering the online milieu (Weimann and Von Knop 2008). Unlike most other models, they do suggest that individuals progress through the stages in a linear manner, noting that it may take weeks, months, or years, while also implying a relationship between engaging with propaganda and conducting plots.

Several commonalities appear when viewing the theoretical frameworks for online radicalisation. Rather than positing a distinct cause and effect phenomenon which explains the process, they tend to propose potential dynamics – typically none of which are necessary or sufficient – that may be either exclusive to, or a prominent feature of, the Internet. This is itself not necessarily problematic, but few of the theories seem to have been developed from empirical research – the exception being Bastug, Douai and Akca (2018) – nor do they appear to be falsifiable in any meaningful way. This is comparable with the wider theoretical research into radicalisation which, as Jensen, Atwell Seate and James (2018) note has not focused on rigorous empirical testing which makes it difficult to judge how well the theories work as general explanations of radicalisation. Rather, they argue that most theories are supported by anecdotal evidence with nebulous selection criteria.

Some online radicalisation theories have been imported from wider social science research and are repurposed as mechanisms for involvement in terrorism. The concept of an online echo chamber is offered explicitly or implicitly (as ideological homogeneity) as a dynamic in most theories. The proposition that individuals select in homogenous groups online is well-established and doing so may have adverse effects on the quality and diversity of information (Bakshy, Messing and Adamic 2015; Del Vicario, Bessi, *et al.* 2016) or that being in one may have negative effects on user sentiment (Del Vicario, Vivaldo, et al. 2016). Research suggests that online activists at each end of the political spectrum are more likely to form echo chambers and less likely to interact with political adversaries (Bright 2017; Krasodomski-Jones 2017). Therefore, there may be some basis for this concern. However, it has yet to be tested on the topic of terrorism or extremism in any robust manner, which leaves little understanding of how this dynamic affects the radicalisation process (O'Hara and Stevens 2015; Whittaker, 2020). Similarly, little attention has been paid to Suler's (2004) online disinhibition effect in the context of terrorism.

Many theories also seem to rest on the assumption that extremist propaganda can play a role in radicalising its target audience. Some theorists, like Koehler (2014), Neumann (2013a), and Ducol et al. (2016) are cautious and equivocate that this relationship is unproven, while others make this relationship a key component to their models (Weimann and Von Knop 2008; Torok 2013; Saifudeen 2014; Neo 2016). The effects of terror propaganda on its audience have only been tested in a small number of studies and suggest that there may be some relationship between engaging with it and supporting a fictional terror group (Reeve 2019), or that if existential threat or uncertainty is primed then it can increase interest or persuasion (Rieger, Frischlich and Bente 2013; Frischlich et al. 2015). However, experimental studies like this are few in number and are not sufficient in recreating the complex personal and social dynamics that go into engagement with terrorism. Models and theories that assume a certain type of message will resonate with their audience without empirical basis are perilously close to rehashing of the now discredited "Hypodermic Needle" model of mass communication, which remains in discussions of terrorist propaganda (Sageman 2014; Archetti 2015; Aly 2017).

The uniting theme between all the theories and models presented above is that they all posit that the online domain is distinct and separable from the offline one. The activity of theorising "online" radicalisation implicitly suggests a meaningful dichotomy between the two domains; the scholars discussed above attempt to show what is distinct about the Internet and why this may result in a markedly different radicalisation process. Several of the authors make explicit mention of the "real world" that can interplay but clearly distinct from the online domain (Weimann and Von Knop 2008; Torok 2013; Koehler 2014; Saifudeen 2014; Neo 2016), with others do not explicitly use this phrase, they still imply a distinction between the two (Sageman 2008; Bastug, Douai and Akca 2018). The dichotomy is challenged by Docul (2015), who critiques existing theories that assume the

two domains are autonomous, yet his proposed SAT framework still necessarily relies on there being a dichotomy, even if they are related.

3.3.3 Ontological Challenges

One common theme from the theories and models of online radicalisation is that they assume there are two distinct spaces – online and offline – that can be separated. In its simplest form, the very notion of "online" radicalisation implies a dichotomy between it and "offline" radicalisation. Even though the research presented above often equivocates by stating that the two are not mutually exclusive and it is rare that an individual engages solely in one domain, it still implies that these are two realities that can be separated. Outside the realm of terrorism studies, this view has been challenged by scholars who believe that the two domains are now inseparable.

This challenge goes at least as far back as the mid-2000s when Floridi (2007) offered a prediction for the future of communication technologies. Arguing that the threshold between online and offline would soon disappear, he notes that the "infosphere" (the whole information environment, the entities that exist within them, and their properties, interactions, processes, and mutual relations) was being re-ontologised due to the convergence between digital resources and digital tools. Importantly, this convergence means that 'there is no longer any substantial difference between the processor and the processed, so the digital deals effortlessly and seamlessly with the digital' (Floridi 2007, p. 60). He argues that this has been caused by two things: Firstly, the transition from analogue to digital data, which has led to a blur between carbon and silicon-based entities. Secondly, this blurring has led to the exponential expansion of the digital space. The implication of this is that human beings will turn into connected informational organisms – "inforgs." These humans will exist in an infosphere which is not merely a virtual environment supported by a material world but rather the world itself will be interpreted and understood as part of a whole infosphere, made up of both the processors and processed, online and offline (Floridi 2007).

The idea of an identifiable online/offline dichotomy is also challenged by Jurgenson (2012) who critiques what he calls "Digital Dualism." He argues that the primary role of communications technologies in the 21st Century have been to effectively link the online and offline domains. Like Floridi, he notes that both spaces enmesh to form an augmented reality; social media supplements our offline lives, rather than replaces them. Offline factors dictate who users are friends with on social media, our social-locatedness, demographics, and epistemological standpoints, which in turn affect online posting behaviours. Conversely, what happens on social media affects how individual act when they are not logged on (in 2021, it is not clear that there is even a state of "not being logged in" for social media users), for example, users are being trained to look for the perfect photo, check-in, or status update even when offline. This is important, Jurgenson argues, because it means that two popular notions of the Internet are fundamentally flawed. Firstly, the techno-utopian view that the Internet could operate as a space which eschewed old oppressive realities, or secondly, the converse argument that the Internet

is the cause of new oppression. On Jurgenson's reading, nothing on the Internet exists outside of longstanding social construction and inequalities.

The idea of the online and offline domains intertwining an in augmented reality is expanded by Rey and Boesel (2014) who argue that we use technologies to express personal agency, potentially experiences online profiles or devices as part of ourselves. They argue that there is a tendency to consider being offline as real and the primordial state of being, which is a naturalistic fallacy as it encourages normative value judgements which dismiss digital interactions, as well as ignoring how interrelated the two domains are in life. They further Jurgenson's (2012) argument by developing the concept of "augmented subjectivity," noting that the online and offline worlds are co-produced and experiences are created simultaneously. Rather than a dualist dichotomy, augmented subjectivity is experienced in both domains as one single, unified reality. This means that contemporary humans are embodied by both organic flesh and "digital protheses" – an extension of the human body in which they can perceive and act in the world. They argue that 'neither the experiences mediated by the subject's organic body, nor those mediated by her digital prostheses can ever be isolated from her experiences as a whole…[they] are always-already inextricably enmeshed' (Rey and Boesel 2014, p. 184).

In recent years, a group of Internet philosophers – led by Floridi – have adopted the neologism "Onlife" to describe this new hyperconnected reality. These scholars argue that it is no longer sensible to ask whether an individual is online or offline, instead positing that communication technologies are environmental forces that affect people's self-conception, mutual interactions, conceptions of reality, and interactions with reality (Floridi 2015). They argue that development in scientific knowledge has brought about a range of technological artefacts that no longer simply operate according to human instructions, but rather 'data are recorded, stored, computed and fed back in all forms of machines, applications, and devices in novel ways, creating endless opportunities for adaptive and personalised environments.' (Floridi et al. 2015a, p.10). This has led to four major transformations: A blurred distinction between reality and virtuality; a blurred distinction between human, machine, and nature; a reversal from information scarcity to abundance; and a shift from the primacy of stand-alone things, properties, and binary relations to the primacy of interactions, processes, and networks (Floridi et al. 2015a).

In contemporary life, the notion of "going online" is a relic of the past in which one needed to make an active decision and dial up a modem on a personal computer. Mobile devices and Internet data mean that people are online almost all the time. Recent reports have suggested that people in the US spend six and a half hours online per day; 82% of the population use mobile devices to access the Internet; and 86% access the Internet every day (Kemp 2019). However, this tells only part of the story; the proliferation of push notifications, which allow for mobile applications to send data to a user's device screen, even if it is not currently running, have been shown to bring users online and increase usage (Stroud et al. 2019). In effect, this means that even when users are not spending over six hours actively online, they are constantly in a state of "online readiness". As well

as this, the relationship of users to the Internet has changed dramatically over the past decade – platforms such as Facebook, YouTube, and Twitter have gone from relative obscurity to become the biggest and most used sites on the Internet. These sites are not like the passive websites of the early Internet in which users gathered information (Sageman 2008a); they are fundamentally social in nature and bridge the online and offline domain.

This Onlife infosphere has important consequences. Thorseth (2015a) argues that it has blurred the traditional distinction between public and private communications has changed; political and public negotiations need not take place in the public space as social media is ubiquitous and what used to be considered intimate (e.g. sexual relations, political affiliations) exists more prominently on public platforms. Public and private should no longer be considered counterparts, but rather complementary categories which are challenged by communications technologies. Ess (2015) expands on this blurred distinction, noting that social media users tend to opt for "publicly private" (revealing one's identity with private content) or "privately public" (not revealing ones identity, but having content public) ways of sharing information online (See also: Lange 2007). Similarly, the new hyperconnected world has changed our social relations; while people used to have a small number of friends located close-by with whom convivial relations were shared, today, the social fabric is dramatically evolving, and people may now be connected with hundreds of even thousands of "friends" or "followers" on social media (Ganascia 2015).

The level of information that is available has dramatically changed too. Broadbent and Lobet-Maris (2015) note that in previous ages, information was scarce, difficult to access and disseminate, but during these times, there was a large capacity to receive it. The hyperconnected Onlife world has reversed this – now there is an abundance of information, but little capacity to avoid it. This has created an economy of attention which is focused on keeping users on social media platforms, but results in volatile and piecemeal identities that lack empathy and a capacity to read others' intentions. Thorseth (2015b) also suggests that, despite the wide access to information, contemporary humans lack the capacity to incorporate diverging opinions, drawing on Sunstein's (2001) concept of a *Daily Me* newspaper in which individuals receive and publish a narrow range of information that coheres to their existing worldview.

Presently, research arguing against digital dualism tends to operate within a broader socio-political sphere rather than focusing on terrorism specifically. Many of these scholars hint at potential security risks that can arise from the re-ontologised world. Jurgenson (2012) argues that his theorised augmented reality is a particularly flammable space. Drawing on the Arab Spring and the Occupy Wall Street protests, both of which highlight the intersection between digital technologies and physical space, he notes that protesters were able to take photos and videos and spread them quickly around the world in participatory prosumer dissent. Protestors also have a much greater audience; rather than merely shouting in the wind, they were part of an interested network which gives

them more motivation to engage with the protest. Thorseth (2015b) briefly discusses the inability to incorporate diverging opinions in the context of Anders Behring Breivik, whose manifesto reflected the vast quantity of information available, but failed to incorporate the perspective of his targets and was therefore an extreme example of Sunstein's (2001) *Daily Me*.

Terrorism scholars have suggested that there may be a false dichotomy between online and offline radicalisation, most notably Gill and colleagues, who note that their empirical results suggest that: 'There is no easy offline versus online radicalisation dichotomy to be drawn. It is a false dichotomy… Often [plotters'] behaviours are compartmentalised across these two domains' (Gill et al. 2015, p. 35). As noted above, Docul (2015) also critiques what he describes as the pervasive assumption that there are two domains – online and offline – that can be easily separated, actions in the two spaces are dynamic and affect the other.

The largest contribution that intersects terrorism and the concept of Onlife is by Valentini, Lorusso and Stephan (2020). They note that many scholars in the field have conceptualised virtual spaces as autonomous from what happens in the "real world" – this type of language is utilised in many of the theories and models laid out above. This, they argue, is a relic of the Web 1.0 in which virtual actions were clearly defined and able to separate from offline ones. However, they note that in contemporary extremism, online and physical spaces conflate in unprecedented ways and should not be treated as separate; 'radicalisation processes evolve, and develop, by integrating elements that pertain to both.' (Valentini, Lorusso and Stephan 2020, p. 12).

They draw on an online structural dynamic – the proliferation of content-sharing algorithms – to demonstrate why terrorism scholars should rethink this dichotomy. Algorithms draw heavily on users' offline resources to perform in the most predictive manner possible; data are accumulated both via online history as well as tracked information as such location, recent purchases, and phone calls. The algorithmic environment is also shaped by negative media diet such as time spent away from a platform and unposted comments (Cohen 2018). The diffusion of portable devices is also important; social media algorithms are continuously structuring an up-to-date datafied image of individuals, even in the so-called "offline" world (Valentini, Lorusso and Stephan 2020). They propose a reconceptualisation to the notion of an echo chamber (posited multiple times above in online radicalisation theories), dubbed an "echo system" in which incorporate both the online elements of alike which engage in a seamless feedback loop with each other. This supports previous research, which suggests that individuals tend to form ideologically homogenous groups offline as well as online (Gentzkow and Shapiro 2011; Pattie and Johnston 2016).

3.3 Two Types of Empirical Research

The field of empirical research into online radicalisation can be divided into two subsections, as formulated by von Behr et al. (2013) in their analogy of the "demand" and "supply" side of a market. They note that the majority of the research into online radicalisation focuses on the supply of potential content which is on the Internet – this could be, for example, studies of propaganda, the dissemination of content, or social network analyses of supporters online. In short, what a would-be terrorist or extremist could plausibly find when on the Internet. However, it is also important to assess how individual terrorist actors engage on the Internet; the *demand* of the radicalisation process. They note that the supply-side is substantially over-represented in academic research:

> The reason for this is relatively straightforward: access to terrorists (those convicted under UK terrorism legislation) or extremists (identified by the police and multi-agency partners based on a risk assessment) willing to speak to researchers is extremely difficult. Access to primary data understandably remains a significant challenge. (von Behr et al. 2013, p.32)

This analogy is also used by Munger and Phillips (2019), who discuss whether YouTube is responsible for far-right radicalisation. They note that despite the supply of content and the affordances that the platform offers – such as recommendation algorithms and the ability to monetise videos – there must still be a demand of users who wish to watch it, regardless of the ease, efficiency, and potency of the content.

The disparity between supply and demand-side research is noted in Gill et al. (2015), who surveyed 200 academic abstracts pertaining to 'online radicalisation' and identified that only 6.5% utilised data of any kind, with only 2% utilising primary data. The difficulty in generating primary data in the radicalisation process produces an over-reliance on secondary sources and anecdotal evidence – both of which have not always been gathered with academic rigour. By comparison, researching the supply-side has low barriers to entry; terrorist organisations tend to make it as easy as possible to access much of their content and many of the most prominent sources for extremism can be accessed easily and without the permission of the author.

Other scholars have addressed this problem, too. Conway (2016a) argues that much of the existing literature studying violent extremists' use of the Internet has focused on analysis of radical content; she suggests that the field needs to "deepen" their endeavours to address this by focusing on the consumers and producers of such content. Aly (2017) also highlights this deficiency in the literature, suggesting that current analyses of extremist propaganda often assume content has a "silver bullet" effect on audiences, and research should seek to answer how and why individuals seek out and engage with such content. Munger and Philips (2019) make a similar point, comparing discussions of radicalisation on YouTube to the now discredited "Hypodermic Needle" model of

communications in which message creates can infect the minds of their passive audiences.

The problem with an over-reliance on the supply-side is that it suggests 'a degree of causality between what is online and the influence on the person reading it, which cannot be proven' (von Behr et al. 2013, p.9). Clearly, there is a benefit to the analysis of the terrorist content available on the Internet, but an over-reliance on the supply side means that there is a strong understanding of what is available, but only unproven postulations as to how it actually affects individuals that become terrorists. The remainder of the literature review will follow this dichotomy. First, an investigation of the demand side; research which analyses how terrorist and extremist actors have used the Internet as they have radicalised. This is followed by reviewing the research into the supply side of IS, where topics such as their propaganda and their online presence are presented. The contribution of this research is to add an empirical insight into the demand-side, for which there is still a dearth of literature, while also using it to draw links with the supply-side by analysing the types of online interactions which actors undertook, such as their consumption of radical content.

3.4 Demand-Side

3.4.1 The Internet is Important

In his 2008 book *Leaderless Jihad*, Sageman argued that the Internet had transformed jihad. He notes that until around 2004, most terror networks were the result of face-to-face interactions, but after, the Internet became the central hub of communications. Previously, he had warned about the potential ways in which the Internet could exacerbate radicalisation, including creating a concrete bond between an individual and their online community which naturally favours radical messages which offer simple solutions, but noted that strong offline social bonds were still vital and these required investment in intense face-to-face interactions (Sageman 2004). However, by the mid-2000s, the dynamics of becoming a terrorist had fundamentally changed and shifted 'from face-to-face interaction at local halal ethnic restaurants or barber shops in the vicinity of radical Islamist mosques to interaction on the Internet' (Sageman 2008a; p.109). While previously he had suggested that radicalisation was caused by small groups of friends becoming progressively radicalised together (his "bunch of guys" theory), he suggests that this now takes place online with online platforms taking the place of radical mosques in previous generations. He goes as far as to suggest that 'face-to-face radicalisation has been replaced by online radicalisation' (Sageman 2008b, p.41).

In the years that directly proceeded Sageman's argument, many other researchers offered support for this position. Weimann (2012) also notes a gradual change from the events of September 11th 2001, in which the Internet provided a paradigm shift. While formal organisations such as al Qaeda present the biggest threat, they had now adapted their modus operandi: 'The real threat now comes from the single individual, the 'lone wolf', living next door, radicalized on the internet, and plotting strikes in the dark'

(Weimann 2012, p.75). He argues that those known as "lone wolves" are rarely alone, but instead learn and communicate with other terrorist actors online. A similar argument is posited by Post, McGinnis, and Moody (2014), who posit that the communications revolution brought about by the Internet and social media has led to a new era of terrorism, creating 'lone wolf terrorists who through the Internet are radicalized and feel they belong to the virtual community of hatred' (Post McGinnis, and Moody 2014, p.306). They argue in particular that diaspora Muslim youth in the West, who do not find acceptance in their homeland, are "radicalised" by online echo chambers because they are accepted in these virtual communities. In their report on U.S. homegrown Islamic extremism, the Anti-Defamation League, concurred with these sentiments, suggesting that 'face-to-face interaction with terrorist operatives is no longer a requirement for radicalization. Individual extremists, or lone wolves, are increasingly self-radicalizing online with no physical interactions with established terrorist groups' (Anti-Defamation League 2014, p.1). These arguments suggest that around the end of the 2000s and beginning of the 2010s, there had been a paradigm shift in radicalisation, and the Internet had become the new norm. It is important to note that the above-mentioned arguments are commentaries or theoretical works, rather than empirical data-driven research. As noted above, the difficulty in generating empirical data has led to an over-reliance on anecdotal evidence when assessing the role of the Internet in cases of terrorism (Gill et al. 2015).

In recent years more data-driven research has been conducted on this topic. Almost uniformly, it points to an important role for the Internet. The report by von Behr et al. (2013) mentioned above, commissioned by the RAND Corporation, remains one of the most important pieces of research on this topic because it utilises primary data. Using a qualitative methodology, they analysed 15 cases of extremism and terrorism in the UK, investigating computer records, evidence presented at trial, interviews with convicted terrorists and with police responsible for counter-terrorism. The researchers conducted a literature review to discern five hypotheses regarding online radicalisation:

1. The Internet creates more opportunities to become radicalised.
2. The Internet acts as an 'echo chamber': a place where individuals find their ideas supported and echoed by other like-minded individuals.
3. The Internet accelerates the process of radicalisation.
4. The Internet allows radicalisation without physical contact.
5. The Internet increases opportunities for self-radicalisation.

The 15 cases studies support the first two hypotheses. They find that 'there is widespread evidence and support for the first hypothesis in the literature. In all of our 15 cases the internet provided the individual in question with a capability to connect, collaborate and convince (von Behr et al. 2013, p.24). They also find that in the majority of cases, the Internet acted as an "echo chamber", in which they could confirm those worldviews with which they agreed, and ignore those with which they did not. There is no support for the final three hypotheses, which will be discussed further below.

There have been a number of quantitative database studies which have analysed terrorists' Internet usage. Gill and others have researched this topic extensively (Gill 2016; Gill and Corner 2015; Gill et al. 2015; Gill et al. 2017; Gil, Horgan and Deckert. 2014). The research seeks to disaggregate the concept of "online radicalisation" into a number of discrete and observable behaviours, which are used as coding points. In their open-source study of UK and US-based lone actor terrorists, Gill and Corner (2015) identify two key ways in which terrorists act online: using the Internet to interact with co-ideologues and learning about or planning their activity. These are then divided into five sub-variables each.[4] They find that 46.2% of terrorists used the Internet to learn or plan their activity online, while 35.3% communicated with co-ideologues online – these findings are also displayed in Gill, Horgan and Deckert (2014). This codebook is used as part of open-source research on a larger sample of 227 UK-based terrorist actors in Gill et al. (2015) and Gill et al. (2017). In total, 61% of cases showed evidence of online behaviours related to the terrorists' eventual activity, with 54% using the Internet to learn about their event and 29% communicating virtually. Importantly, data collection included cases from 1995-2015, but when the date range is narrowed to 2012-2015, the number that used the Internet to learn about their activity rises from 54% to 76%, suggesting a greater reliance on the Internet than in years previous. Gill (2016) also uses this coding system to conduct closed-source research on UK-based lone actors, finding that 59.2% of actors used the Internet to interact with co-ideologues online and 81.6% used the Internet to learn about or plan their activity.

Beyond presenting descriptive statistics, Gill and others also conduct bivariate analyses which offer an important insight into how the Internet is being used by terrorist actors. For example, Gill et al. (2017) find that those that plotted to use an IED were 3.34 times more likely to have learned online, which they argue reflects both the complexity in creating a bomb as well as the relative ease with which bomb-making instructions can be found online. They also find that lone actors were 2.64 times more likely to learn online than those who were part of a cell, which indicates that lone actors lack the human, social, technical, and financial capital and aim to supplement it by learning on the Internet (Gill et al. 2017). Furthermore, they find that those that plotted to attack government – rather than civilian – targets were 4.50 times more likely to use the Internet to learn, pointing to the greater degree of risk involved which requires the need to go online and learn (Gill et al. 2017). Finally, they find that far-right terrorists were 3.39 times more likely to learn online than jihadist terrorists, suggesting that the former is more dependent on the cyber realm in the UK. These studies by Gill and others, taken together, show that between a sizable minority and a majority of terrorist actors use the Internet as part of their activity. Furthermore, the number may be growing as we enter an age of greater cyber-

[4] For online interactions with co-ideologues: a) Reinforce prior beliefs; b) Seeking legitimization; c) Disseminating propaganda and providing material support; d) Attack signalling; and e) Attempting to recruit others. For learning about or planning their activity online: a) Access ideological content; b) Opting for violence after witnessing something online; c) Target selection; d) Preparing an attack; and e) Overcoming hurdles.

dependence; and that there are specific affordances that terrorists are able to utilise via the Internet.

A number of other database studies have sought to assess the role of the Internet in cases of terrorism. Woodring (2014) analyses 331 individuals engaged in pre-incident planning processes between 1995 and 2011 in the US to discern the role of the Internet in the radicalisation process. He finds that 55% of the cases were found to have clear evidence of Internet usage, of which communication with other extremists was the most prevalent (42.9%), followed by information gathering (35.6%), and then propaganda (32.3%). Horgan et al. (2016) also use a US-based dataset with a similar timeframe (1995-2012), finding that 42.1% of actors expressed their ideology online, and only 13.5% did so exclusively in the online domain. Unlike the studies of Gill and others, there is no filter for more recent years, so it is impossible to tell if the Internet has become more prevalent in these samples. That being said, the findings still show that a sizable minority of actors used the Internet during this timeframe, suggesting it is an important tool for terrorists' communication and event planning.

More recently, Bastug et al. (2018) conducted open-source research to create a database on 51 Canadian terrorists. They found that data relating to actors' radicalisation – which appears to mean their activity prior to showing outward support for a terrorist ideology – was available for 32, and the data show that the Internet played a role for at least 21 of them, leading them to the conclusion that at least 41% were, at least partially, radicalised online. Moreover, actors continued to use the Internet after accepting the ideological worldview: 'The results of this study demonstrated that social media and the Internet played a role either during or after the radicalization process of at least 76 percent of the sample' (Bastug et al. 2018, p.16). They posit a four-step radicalisation process which the actors in the sample followed: Firstly, accessing extremist content online, then secondly, engaging a pre-disposition or susceptibility to extremist messaging resonating, before, thirdly, moving to mobilise with terrorist groups and proselytising for them, before finally going back to social media to share their experiences, creating a feedback loop which creates new extremist content (Bastug et al. 2018).

Other research on terrorism in the US has posited an important role for the Internet, too. Using the Profiles of Individual Radicalization in the United States (PIRUS) dataset, Jensen, James, et al. (2018) find that actors' usage of the Internet has steadily grown in recent years. From 2005-2010, they find that only a quarter used social media, it only accounted for a primary role in radicalisation in around 1% of cases. In the years 2011-2016, this had switched to around 75% using social media – although it was only deemed a primary part of the radicalisation process in 17% of cases (Jensen, James, et al. 2018). In the years 2015 and 2016 alone, they find that around 85% of actors used social media. They also posit that the duration of the radicalisation process of the individuals in their sample was substantially shorter in these periods of higher social media usage than earlier in the dataset, suggesting that the Internet may shorten the period in which it takes an actor to radicalise (Jensen, James, et al. 2018). The notion of social media being

important in cases of terrorism in the US has also been posited elsewhere. In their study of the flow of foreign fighters to jihadist groups – including IS – in Syria and Iraq, the Soufan Group (2015) note that for most countries, pre-existing offline networks drove mobilisation, but actors leaving the US had been reliant on social media for recruitment to the group.

Although quantitative research can offer important insights into how many actors used the Internet, it can also fall short of offering an in-depth picture and nuance. Koehler (2014) conducted qualitative interviews with eight far-right extremists, four of whom were radicalised before the rise of the Internet and four after, applying a grounded theory methodology to discern the role of the Internet in the radicalisation process. He offers a number of key findings. Firstly, that the Internet is useful in providing an efficient and cost-effective means of communication, networking and organisation which leads to better integration – with a forum administrator estimating that 70-80% of networking is done via the Internet. Similar arguments of ease, efficiency, and cost effectiveness are made regarding jihadist terrorism by the Institute for Strategic Dialogue (2011). Importantly, the online social structures of these networks translate into offline status, suggesting that the communication that was taking place online had real impact (Koehler 2014). Secondly, he finds that the lack of constraint informed by perceived anonymity was found to have a core radicalising function. Interviewees remarked on a separate online persona that was entirely different, and often more "ideologically pure", than offline (Koehler 2014). This is a finding that has also been posited when discussing jihadist extremism online. Brachman and Levine (2011), note the flexibility of constructed identities in cyberspace allows would-be terrorists to create "avatars" which are more radical than their offline counterparts.

Koehler's third finding is that the Internet provided an opportunity for ideological development with a potentially unlimited number of individuals, which offers the movement the chance to become aware of those who do not necessarily agree (Koehler 2014), which is similar to the point made above by Sageman (2008a), that dissenting voices either leave or are cast away and the movement is shaped by those who remain on message. Fourthly, Koehler (2014) finds that the Internet offers the perception that the movement was bigger and more successful than it actually was – also corroborating the claims of Sageman (2008a) and has been empirically tested on a neo-Nazi online forum by Wojcieszak (2008). Koehler argues that this motivated individuals in the movement to become further involved or act more radically. Finally, he found that that for the younger interviewees, they found contact with the movement *before* they had any offline contacts. As a result, it created a critical mass effect, which:

> Provided an image of a right-wing movement that might convincingly be able to take over power or reach its goals. This, in turn, encouraged some of the interviewees to get more involved and, consequentially, seek offline contacts…They have been indoctrinated and socialized online before they were integrated into offline structures or activities' (Koehler 2014, p.121)

The finding that the Internet may provide an entry point to new recruits is something that is hypothesised more broadly than the far-right movement by Holt et al. (2016) who argue that although would-be extremists come to the movement from several different avenues, the Internet may provide a common entry point.

Although Koehler's research is focused on a small sample size and relates only to neo-Nazis, it is an important contribution to the research because it offers a number of important qualitative hypotheses in a field which contains mostly – save the von Behr et al. (2013) study – quantitative research. Furthermore, the research seems to corroborate claims made by scholars within terrorism studies. Koehler's research suggests that because of these findings, these individual's radicalisation was shaped, or even made possible by the Internet (Koehler 2014).

Pauwels and Schills (2016) take a survey-based approach to attempt to understand the relationship between exposure to extremist content and self-reported. They conduct both an offline survey of 16-18 year old Belgians in school and an online survey of students and young adults that have left school, creating a total response of over 6,000 respondents. Although they only found small support for violent extremism (2.4%) and actually engaging in political violence (3.3% at least once and 0.2% more than three times), around half said they had been exposed extremist content on social media, with 1.6% saying they were exposed to it daily. Importantly, they find a positive relationship between consuming extreme content and self-reported political violence and those that actively sought such content were more likely to engage in violence than those who passively consumed it. Their findings still stood when controlling for a range of variables from competing theories such as religious authoritarianism, thrill-seeking, and perceived personal discrimination (Pauwels and Schills 2016).

Other research has sought to analyse the role of the Internet via individual terrorist actor case studies. While one should be careful not to over-interpret individual case studies, they can be important in adding in-depth perspectives to actors' trajectories. In her study of the case of Roshonara Choudhry, who stabbed British MP Stephen Timms in 2010, Pearson (2016) notes that the Internet may have provided a space for her to construct a less-restricted gender identity; women are generally precluded from fighting in Salafi movements, but Choudhry's apparent social isolation allowed her to move from this view to a more ambiguous perspective which offered an alternative agency for women. Similarly, Picart (2015) notes that the Internet aided the radicalisation of Colleen LaRose because it permitted her to construct an online identity that eschewed these traditional Salafi gender roles and ultimately led to her involvement in the plot to murder Danish cartoonist Lars Vilks in 2009, although the role of the Internet is downplayed to some extent in another study by Halverson and Way (2012), who do note the importance of the web, but emphasise that her personal history and the stressors she experienced may be more important.

Taken together, these findings paint a relatively cogent picture. First and foremost, the Internet is used by terrorists, either by a majority or a sizable minority. This does perhaps suggest that the claims above by Sageman (2008b) that face-to-face radicalisation has been replaced by online radicalisation may be slightly over-cooked given that only a small number of studies show that an overwhelming majority used the Internet. However, the Internet is clearly important and more recent studies show a higher usage. Secondly, the research presented above shows that the Internet provides a number of opportunities and affordances – the von Behr study (2013) and the research by Gill and others (Gill et al. 2015; Gill et al. 2017; Gill 2016; Gill and Corner 2015) all find that terrorists are using the Internet for a multitude of different behaviours. Finally, the studies by Koehler (2014), Pearson (2016), and Picart (2015) suggests that there are online dynamics in actors' subjective lived experiences, beyond the reach of quantitative research, that may exacerbate an individual's pathway towards extremism.

3.4.2 Downplaying the Role of the Internet

The empirical research presented above points to the Internet being an important part of contemporary pathways towards terrorism. In most cases a majority of terrorist actors use the Internet and do so using a number of different affordances, including communicating with ideologues and planning. Furthermore, there is evidence to suggest that the usage of the Internet may be growing over time. However, it is prudent to ask whether one should be surprised that the Internet is utilised highly by terrorists. In his assessment of why the Internet is not increasing terrorism, Benson (2014) notes that the Internet is the dominant mode of communication of this period of time and it would be strange if terrorists were not using it. However, he challenges the causal logic that it necessitates some kind of new threat. This point is also made by Neumann (2013a), who argues that there is nothing unusual about terrorists using the Internet, nor is there anything surprising about how they use it: 'Like everyone else, they disseminate their ideas and promote their causes, they search for information, and they connect and communicate with like-minded people, often across great distances' (Neumann 2013a, p.433). Although the perspective offered above does suggest a central role for the Internet in cases of radicalisation, there is another perspective, which does not dispute this, but argues that when considering other factors – particularly offline interactions – the Internet is less important than those like Sageman (2008a) suggest.

In their study, von Behr et al. (2013) find that each of their actors used the Internet and it offered affordances that helped them along their pathway, but did not find support for three other hypotheses:

3. The Internet accelerates the process of radicalisation.
4. The Internet allows radicalisation without physical contact.
5. The Internet increases opportunities for self-radicalisation.

For number 3, they argue that it is too difficult to judge this phenomenon because of the lack of data into how long a radicalisation trajectory should take (von Behr et al. 2013).

The lack of evidence for numbers 4 and 5 are particularly important in the study of "online radicalisation"; they find that, in most cases, both online and offline factors play an interconnected role in actors' trajectories and that acting in the two domains complement each other. They similarly find that there is no case to be made for "self-radicalisation" as actors remained in contact with other individuals, both online and offline (von Behr et al. 2013). They conclude that:

> The internet has to be seen as a mode, rather than a unitary method, of radicalisation (the internet can play an important role in facilitating the radicalisation process; however, it cannot drive it on its own). Instead, the internet appears to enhance the process (von Behr et al. 2013, p.33)

That is to say, they downplay an online radicalisation thesis. The Internet offers affordances and operational benefits which may develop the process, but actors are not reliant on the online domain.

This perspective is mirrored in the work of Gill and others (Gill 2016; Gill and Corner 2015; Gill et al. 2015; Gill et al. 2017; Gill, Horgan, and Deckert 2014). Although the findings do suggest that most terrorists use the Internet for a number of different behaviours – and prevalence is rising as time goes on – the studies also code for a number of offline behaviours and subject them to bivariate tests. Gill et al. (2017) find that the learning or planning of terrorist activity online was strongly correlated to offline behaviours: 'Those who learned online were 4.39 times more likely to have experienced nonvirtual network activity and 3.17 times more likely to have experienced nonvirtual place interaction' (Gill et al. 2017, p.110). Similarly, those that communicated with ideologues online were significantly more likely to engage in the offline domain: 'Those who communicated online were 3.89 times more likely to have experienced nonvirtual network activity and 3.17 times more likely to have experienced nonvirtual place interaction' (Gill et al. 2017, p.110). Similar results are found in Gill and Corner (2015) and Gill (2016). Gill et al. (2017) note that their findings are in line with the von Behr (2013) study:

> The Internet is largely a facilitative tool that affords greater opportunities for violent radicalization and attack planning. Nevertheless, radicalization and attack planning are not dependent on the Internet and researchers need to look at behaviors, intentions, and capabilities. (Gill et al. 2017, p.113)

Importantly, they argue that the online/offline dichotomy of radicalisation may be a false one because plotters tend to act in both domains, meaning that there is often no easy distinction to be drawn (Gill et al. 2017).

Hussain and Saltman (2014) offer a mixed method study, commissioned by the Quilliam Foundation. It includes interviews with experts, target audiences, as well as data collected from websites, social media, and fora. They too, find that the Internet is an important tool in contemporary radicalisation. However, they also observe that 'there is

little to no evidence showing that individuals are radicalising online without any contact or information given prior by real-world interactions or experiences' (Hussain and Saltman 2014, pp.80-81). They note that the Internet is important in three key ways: indoctrination, teaching, and socialisation, but that the 'vast majority…come into contact with extremist ideology through offline socialisation prior to being further indoctrinated online' (Hussain and Saltman 2014, p.7). The finding that actors come into contact with ideology offline first is important because it offers an opposing view to that laid out by Koehler (2014) above, who finds that for younger members, the Internet was often the entry point for actors.

The importance of offline interactions is also highlighted in several other studies. Reynolds and Hafez (2017) create a database of 99 Germans that travelled to Syria and Iraq using open sources. They then test three hypotheses to explain what drove their mobilisation: a lack of integration, online radicalisation, and peer-to-peer offline networks. They find only modest support that the travellers lacked integration and meagre support that actors were radicalised online; they narrow the latter down to a maximum of twenty, but there are more likely between 4 and 7 cases that were driven by social media (Reynolds and Hafez 2017). Importantly, they find strong support that offline social networks played a driving role – 80% of their sample was mobilised within an interconnected network and the mobilisation was geographically clustered, not diffused, as one might expect if the Internet played a driving role (Reynolds and Hafez 2017). The notion of "radicalisation hotspots" – i.e. areas that produce a far greater number of Islamist terrorists than one would expect given local Muslim populations – has been posited by a number of scholars in the literature, with examples including Minneapolis, MN in the US; the Molenbeek area of Brussels, Belgium; and the district of Fredrikstad in Norway (Vidino et al. 2017; Varvelli 2016; Soufan Group 2015). As Reynolds and Hafez (2017) suggest, they run as an interesting counter-hypothesis to online radicalisation as one might expect mobilisation to be more, or even completely, evenly distributed if the Internet was a driving force; after all, it can provide actors the ability to communicate across the world with co-ideologues at almost no cost. Rather, the existence of hyper-local interactions at the community level suggests that it is offline interactions which remain most important. However, this research seems to posit a sharp online/offline dichotomy, which is challenged by a number of scholars and this research's findings.

Studies on the foreign fighter phenomenon have also downplayed the role of the Internet. The above-mentioned report by the Soufan Group (2015) does signal out the jihadist mobilisation from the US to the caliphate as being reliant on social media. However, this is mentioned as an outlier to the rest of the world. They note that in countries with the largest flow of fighters, recruitment was localised and few left on their own. Instead, friends and family played important roles. The report does comment on IS' sizable and sophisticated media outreach, but notes that it is intertwined with peer-to-peer persuasion offline, pointing to the latter as a better explanation or mobilisation (Soufan Group 2015). A report for the United Nations Counter Terrorism Executive Directorate

highlights that social media is important in cases of foreign fighter travel, suggesting that it may strengthen and shorten the process – although evidence for these two claims is not provided – but also highlights that mobilisation still seems to rely on physical contact (UN CTED 2015). In interviews with 43 returning foreign fighters, El-Said and Barrett (2017) note that social and personal offline networks were key mechanisms in the evolution of actors' trajectories. The respondents were conflicted as to the importance of the Internet with eleven saying it was either very or extremely important, nine saying it was not important at all, and eleven stating that they were unsure (El-Said and Barrett 2017). Several respondents said they first developed the idea of travelling offline before turning to the Internet to reinforce this notion with communications or propaganda, which supports the findings presented above by Hussain and Saltman (2014).

The interconnected nature of the online and offline domains is further shown in Baugut and Neumann's (2019) study on the use of online propaganda. They conduct interviews with 44 former Islamists regarding their consumption of propaganda and find that it happened both via the Internet and personal talks without the use of media. Actors would watch online propaganda and then discuss it with peers and preachers in an offline setting, and vice versa; discussions with friends and at mosques would lead them to watch propaganda online afterwards (Baugut and Neumann 2019). Notably, the research suggests that actors used a particular affordance of social media – recommender algorithms – to "incidentally" encounter Islamist propaganda and that they say it resonated heavily with them. Other research has suggested that these algorithms may promote interactions with further extreme content after a user begins to interact with them (O'Callaghan et al. 2015; Reed et al. 2019; Ribeiro et al. 2019). Despite this, they suggest, like Gill et al. (2017) and von Behr et al. (2013), that demarcating between the two domains is not a useful conceptualisation because the two modes of communication are strongly intertwined.

Research analysing the US specifically has also highlighted the importance of offline networks. The above-mentioned work by Jensen, James, et al. (2018) highlights the high social media usage of radicalised individuals, but note of the almost 77% of those that did, did so to supplement face-to-face interactions with other extremists. In their report on IS in the US, Vidino and Hughes (2015) stress the important of online interactions, suggesting that there is a cyber footprint in most cases. However, they warn against over-emphasising this role; in most cases, online and offline dynamics complemented each other. Similarly, in their report on travellers from the US to the caliphate, Meleagrou-Hitchens et al. (2018) do point to the importance of social media and online propaganda, but note that in most cases, a range of online and offline factors pushed individuals to travel and that 'there are very few cases wherein a traveler radicalized, decided to travel, traveled, and reached their destination without any offline connections' (Meleagrou-Hitchens et al. 2018, p.6). This view is also echoed in Alexander's (2016) case study-based research of 25 female American IS actors; she notes that most used social media and it was an important way in which they contributed to the online radical milieu. However, this was complemented by several offline dynamics too. Even if, as the Soufan Group's

(2015) report suggests, US travellers were reliant on social media, this does not seem to have come at the expense of offline interactions. Rather, as the research by von Behr et al. (2013) and Gill et al. (2017) suggests, the two can complement each other.

Holbrook has conducted several pieces of research using closed-source data on the media consumption of convicted British terrorists (Holbrook 2017a; Holbrook 2017b; Holbrook 2019). Although the research does not explicitly analyse Internet-usage, focusing both on online and offline media, it offers an important perspective on a key point in online radicalisation. One of the five hypotheses of the Von Behr et al. (2013) study is that the Internet may act as an echo chamber; a place in which radicalising individuals can select perspectives which agree with their worldview and ignore those that do not, which may lead to the normalisation of violence. Pertinently, Sageman (2008a) argues that moderates will leave the online community, leaving only the most extreme perspectives. Holbrook's research offers an empirical view that is somewhat at odds with this argument. Using a multi-level "extremist media index", he finds that the plurality of media that was collected by convicted terrorists was, in fact, moderate in nature including some which actually dissuaded against violence, as well as day-to-day religious concepts and etiquette guidelines (Holbrook 2017b). This suggests that the convicted terrorists in this sample do not merely opt for the most extreme material available and are willing to entertain cross-cutting points of view, although it should be noted that the research analyses the content which terrorists collected, not necessarily what they actually consumed.

The empirical findings presented above offer two perspectives. Firstly, that the Internet is important in pathways towards terrorism – actors, particularly those closer to the modern day, tend to use the Internet for several behaviours, including communicating with co-ideologues, consuming propaganda, and planning their events. Secondly, other factors, particularly offline interactions still play a vital role in contemporary trajectories. These two perspectives are not necessarily in conflict; there is no contradiction in the idea that the Internet has become more important, but has not replaced offline socialisation. However, the second empirical perspective does depart from the commentary offered by the likes of Sageman (2008a), Weimann (2012), Post, McGinnis, and Moody (2014), and the Anti-Defamation League (2014), who posit that face-to-face interactions *have* fallen by the wayside in place of online activity. This, it seems, has little support in the empirical literature. That being said, other perspectives that highlight a potential online radicalisation thesis do emerge from the literature. For example, the idea that actors may construct an idealised persona online that is ideologically pure; or that the Internet may provide the first steps into the radical milieu; or that it provides specific affordances, such as the ease of access to bomb-making instructions, communications around the world, or recommendation algorithms that drive users further towards radical content. There is little consensus on what actually constitutes online radicalisation, but there are a number of concerning signs that the Internet may exacerbate the process.

A final point to mention is that almost all of the research into the "demand-side" is focused on populations within Europe and North America. This is important both because it may represent an Anglo-centric bias towards knowledge and methods of research, as well as the fact that other parts of the world have fundamentally different access to the Internet. The role of the Internet in pathways towards terrorism in America may be substantially different to the Philippines, Mali, or Chechnya.

3.5 Supply-Side

The previous section presented literature on the demand side of online radicalisation research; that is to say, how individuals use the Internet as part of their pathways towards terrorism or extremism. Although many important inferences can be drawn from this research, it is also important to review research which relates to the content that those individuals could interact with online, particularly to assess whether it informs the findings of the demand side. Given the sheer volume of supply side research in this field – the von Behr et al. (2013) study notes that it is dramatically over-represented in their literature review – what follows below will narrow itself in scope to the online activities of IS and related topics. It focuses on two interrelated themes: literature on the group's propaganda and research analysing its exploitation of social media platforms.

In both cases, the literature maps out a period of ascent in which the group and its supporters were able to create a high quantity and quality of content and disseminate it effectively on social media. Furthermore, in both instances, there was a period of decline in which the group found it difficult to create and disseminate propaganda as well as finding a more hostile online ecosystem, causing the online radical milieu to become more sophisticated in their use of the Internet. This chapter explores how these changes have affected the supply of content available online. Furthermore, themes such as understanding the online space as a gendered one; the importance of low-level "cool" peer-to-peer content; and recognising the knowledge gap created by lop-sided research into one platform. Given that the group is repeatedly noted as having sophisticated propaganda and wide-reach on social media, this logically leads to the question of online radicalisation – if there is a relationship between acting in the online radical milieu and engaging in acts of terrorism, a sample of IS terrorists is a worthwhile place to investigate.

3.5.1 Islamic State Propaganda Strategy

IS came to global prominence in the summer of 2014 with its capture of Mosul, Iraq's second city and with it, its declaration of a worldwide caliphate (Whiteside 2016). At the same time, the group's propaganda also caught attention as it released gruesome execution videos, like that of Mohammad Emwazi decapitating American journalist James Foley in August of that year (West 2016). However, the academic literature shows that IS' propaganda strategy is considerably more nuanced than execution videos. In the summer of 2015, Winter collected over 1000 pieces of IS propaganda, which included videos, photos, infographics, news bulletins, and theological essays. He finds that the group was conducting an exceptionally sophisticated strategic communications

operation, both in terms of quantity and quality (Winter 2015b). Rather than the sheer brutality of videos like Foley's execution, Winter finds six themes in the propaganda: mercy, belonging, brutality, victimhood, war and utopia. The final theme – utopia – which depicted life in the caliphate as an actualised vision, accounted for over half of the total propaganda output. The IS "brand" is fundamentally a state-building exercise (Winter 2015b). Elsewhere, he finds that the group's central media office thoughtfully and tirelessly promotes "media jihad" in a concerted effort to build their brand – to the point that the production and dissemination of propaganda is at times considered to be more important than military jihad (Winter 2017).

Other scholars have highlighted the group's sophisticated propaganda operations too. Zelin (2015) analyses a corpus of IS messages in the spring of 2015 including pictures, infographics, news reports, radio broadcasts, and videos. He finds, like Winter (2015b), that the group produces a very large quantity of messages and that the campaign is sophisticated. Also like Winter, his study shows that execution videos make up a relatively small proportion of the total number, relying heavily instead on 'productions on military affairs, governance, preaching, moral policing, and other themes' (Zelin 2015, p.85). Pelletier et al. (2016) argue that IS has been the most effective violent extremist organisation at crafting and disseminating strategic communications for the fulfilment of their objectives. Their study focuses on the role of religious scriptures on messages, finding a number of tactics, including stressing the historical precedent when their position is consistent with mainstream Islamic law; obfuscating differences when it is not; and reinterpreting Islamic law until it is consistent with their strategic goals (Pelletier et al. 2016). This view is echoed by Farwell (2014), who notes that IS stands apart from other groups because of its sophisticated propaganda which aims to persuade Muslims that fighting for IS is a religious duty and portrays the group as an agent of change and a champion of social justice that will ultimately be victorious.

Ingram (2015) also argues that IS information operations are sophisticated; the group seeks to create a dichotomy between friends and foes and in doing so polarise support for the group. He highlights two important, concurrent themes. Firstly, messages appeal to pragmatism, promoting themselves as stable and strong, while highlighting opponents' weaknesses and drawing on the difference between their words and actions. At the same time, messages draw on emotional and perceptual factors such as the identity of the in-group and out-groups, attempting to make their audiences choose between "us" and "them" (Ingram 2015). Importantly:

> IS communiqués rarely appeal to pragmatic or perceptual factors in isolation. Rather, these appeals are woven together into narratives that are reinforced by emotive imagery and powerful symbolism. This approach imbues IS messaging with a greater potential to resonate with the broadest spectrum of potential supporters. (Ingram 2015, p.376)

Both Ingram and Winter show that rather than zealously preaching or showing brutal propaganda – the IS media strategy is highly developed and deliberate and has the potential to resonate with audiences.

3.5.2 Videos

After the group rose to prominence in the summer of 2014, many scholars commented on the high-quality and "Hollywood-esque" nature of the videos (Shehabat and Mitew 2018; Hafez and Mullins 2015; Lakomy 2017a). Winter (2015a) offers an in-depth analysis of the propaganda video *Although the Disbelievers Dislike It*, which shows the execution of twenty-two Syrian hostages followed by Mohammad Emwazi announcing the death, and standing over the head, of Peter Kassig, an American aid worker captured by IS. Although Winter highlights a number of mistakes and inconsistencies when inspecting closely, he emphasises the impressive production quality, noting that the video took from four to six hours to shoot; that there was evidence of multiple takes; and that the group invested a considerable amount of capital into it (Winter 2015a). He notes that 'the production effort behind *Although the Disbelievers Dislike It* was formidable. It is clear that the content of the video was carefully considered and the individual (or individuals) who directed it were obvious perfectionists' (Winter 2015a, p.31). The sophistication of IS videos is also highlighted by Botz-Bornstein (2017), who notes that the group utilise a "futurist" aesthetic in their propaganda, drawing an example of *The Flames of War*, an hour long propaganda video. He notes that 'A futurist touch is also achieved through a willfully colorful and fragmented presentation of reality… the color is so saturated that the combatants appear to glow with light' (Botz-Bornstein 2017, p.4). This aesthetic, he argues, helps transmit the idea of a distinct and pious lifestyle that the "warrior" should adopt (Botz-Bornstein 2017).

IS' video production quality did, however, not remain at this high-quality level. As the group lost its once-substantial territory in Syria and Iraq it took a substantial toll on its ability to continue investing in the same level of propaganda. In agreement with those above, Lakomy (2017a) notes that IS' most influential and successful pieces of propaganda were the videos created in 2014 and 2015, 'All of them were of the highest technical quality and contained sophisticated manipulation techniques' (Lakomy 2017a, p.43). However, he notes that in 2016 and 2017, the quality regressed substantially, with the newer videos containing editing, montage, and post-production mistakes, suggesting a lack of care before final rendering, which he argues, would have been unthinkable in 2014 and 2015 (Lakomy 2017a). In his study of the 772 official videos which the group released from 2015-2018, Nanninga (2019) finds that the production quality declines substantially. This, he argues, works in tandem with the group's rise and fall; their expansion was coupled with an extensive and unprecedented media effort in the region, but the collapse of the caliphate strongly affected the quantity and quality of content. Robinson and Dauber (2018) also highlight the substantial difference between the high quality video productions up until the autumn of 2015, at which point it took a severe debilitation, although they argue that it began to rebuild in quality again in 2016. Each of

the authors presented in this and the previous paragraph agree that the group's video propaganda output in and around the summer of 2014 was high quality and high volume. Furthermore, it is not an exaggeration to suggest that these videos played a large part in the building of the IS brand. Although the quality did not last, as demonstrated by Lakomy (2017a), Nanninga (2019), and Robinson and Dauber (2018), it is possible that it helped influence many adherents to the group in the initial period.

3.5.3 Magazines

Another hallmark of IS propaganda are the e-magazines that the group created and disseminated. However, in this instance, it is instructive to look briefly at what came before it – al-Qaeda in the Arabian Peninsula's (AQAP) *Inspire* magazine, both because it retains substantial support amongst English-language IS supporters (Vyas 2017; Shane 2016a) and because much of the literature on IS magazines is comparative with *Inspire.* One important point made by Sivek (2013) is that *Inspire* deliberately sought a Western English-language audience by delivering the content in a lighter tone, employing "superhero" narratives, using rap lyrics, and telling satirising jokes. This was, according to Sivek (2013), calibrated to ease a potential recruit's passage through the radicalisation process. This notion is expanded upon by Lemieux et al. (2014) who argue that *Inspire* is aimed at a less intellectually informed and engaged audience, choosing statements from figures from the Western world such as Barack Obama, Julian Assange, and Faisal Shahzah. The magazines use stories of martyrdom and the conceptualisation of war between Islam and the West to evoke guilt in readers, and importantly, offer the reader the skills to act upon this with its *Open Source Jihad* section, which would contain instructional material (Lemieux et al. 2014; Conway, Parker and Looney 2017). The Western-oriented focus was not, according to Droogan and Peattie (2016) a constant. Rather, *Inspire* was dynamic, switching focus as global events changed, such as the Arab Spring in 2011, showing an awareness and a willingness to change their strategy to capitalise on important news within their target audience's community (Droogan and Peattie 2016).

IS created several different e-magazines in recent years, most notably *Dabiq* and its successor *Rumiyah*, but also *Dar al-Islam, Islamic State Report*, and *Islamic State News,* which had shorter runs. Novenario (2016) offers a comparative analysis of *Dabiq* with two AQAP magazines (*Inspire* and *Resurgence*) to determine the strategic logic employed by each. She finds that the two groups' priorities are converse: AQAP focuses on the "far enemy" – the West, and seeks to influence policy and behavioural change by attrition, with an end goal of building a caliphate. *Dabiq*, on the other hand, shows IS' strategy to be a state-building enterprise – which is congruous with the findings presented above by Winter (2015b) – which will later result in an end of days war (Novenario 2016). Although *Dabiq* did encourage lone actor attacks, the priority was to bring as many travellers to the caliphate.

In his analysis of *Dabiq*, Ingram (2016a) shows that the magazine aims to show the reader that IS will solve the personal and collective crises of the Sunni Muslim in-group. The out-

group "others" – the West, Jewish people, Shia, and moderate Muslims are rarely linked to these crises without the group describing how it will alleviate it. Unlike *Inspire*, Ingram notes that *Dabiq* does not offer operational advice, but instead retains a persistent message that Sunni Muslims are in a persistent war, leveraging a black and white choice with its audience (Ingram 2016a). The notion of "othering" the West in *Dabiq* and *Inspire* is explored by Lorenzo-Dus and Macdonald (2018), who conduct a corpus linguistic analysis of both magazines. They show that the two both use specific textual strategies to construct the West as an "other" by homogenising it, then suppressing it via negative stereotypes, before finally subjecting it to pejoration (Lorenzo-Dus and Macdonald 2018). Other studies have focused on the "us" vs "them" nature of *Dabiq*; Lorenzo-Dus et al. (2018) draw on the distinction between jihadism and the West, in agreement with Ingram (2016a); while Wilbur (2017) focuses on the magazine's attempt to "outbid" rival groups like AQ, a sentiment shared by Novenario (2016).

Dabiq was replaced by its successor *Rumiyah* in September 2016 – possibly because of the group's imminent loss of the town of Dabiq in Northern Syria. Ingram (2018) observes that the military losses were causing a noticeable decline in quality in *Rumiyah* compared to its predecessors, in agreement with the analyses of video content by Lakomy (2017a), Nanninga (2019), and Robinson and Dauber (2018). He also argues that the tone of the magazine reflects this, such as the suggestion that the current hardship which the group were undergoing were divine gifts to purify its ranks (Ingram 2018).

The inclusion of a section devoted to instructional material – called *Just Terror* is relevant, too; he argues that it represents an important shift from their state-building brand which was less credible given their territorial losses (Ingram 2018). The *Just Terror* section, as Reed and Ingram (2017) find, advises far simpler attacks than *Open Source Jihad* in *Inspire*, suggesting knife, vehicle, arson, and hostage attacks – drawing a potential link between them and the attacks in Berlin, Westminster, and Stockholm, although conceding that finding a causal link is not possible. Wignell et al. (2017) find that although there are many similarities that remain constant in both *Dabiq* and *Rumiyah*, such as their core values, antagonism, and intolerance, they note that their communications strategy from the latter changed with their fortunes on the battlefield. As they were expanding, their focus was on migration, recruitment, and state-building, but as they were declining the focus switched to affiliated organisations in Africa and inspiring lone actor attacks (Wignell et al. 2017). Just as with video content, a clear trajectory can be seen for IS publications, both in terms of quality and content. As the group was expanding, it was producing high quality magazines which sought to sell the caliphate as a legitimate state, but as it declined, it attempted to shift focus away from Syria and Iraq as the quality simultaneously diminished.

Another important theme in jihadist magazines is their use of images; Macdonald and Lorenzo-Dus (2019) conduct a news value analysis of five magazines – AQAP's *Inspire* and *Jihad Recollections*, al Shabaab's *Gaidi Mtaani*, the Taliban's *Azan*, and *Dabiq*. They find, as with studies mentioned above, that the magazines lean heavily on in- and out-

group dynamics and that the non-IS magazines focused on singular individuals, but *Dabiq* focused on groups undertaking collective activities, in line with their caliphate-building ideology (Macdonald and Lorenzo-Dus 2019). Importantly, all five magazines, including *Dabiq*, constructed the aspirational identity of what they call the "Good Muslim", a respected non-leader figure who would hold weapons and other artefacts, and rarely experiences negative emotions (Macdonald and Lorenzo-Dus 2019). Winkler et al. (2018) analyse the use of images of death and dying in *Dabiq* and IS print publication *al Naba*, finding that the group rely heavily on images of enemies who are about to die to demonstrate their military strength and willingness to protect the caliphate. At the same time, pictures of the dead in *Dabiq* differ depending on the identity of the deceased; bodies of dead civilians are displayed disrespectfully, while the bodies of IS martyrs are typically cleaned before being photographed (Winkler et al. 2018). Finally, in their study of child images in jihadist magazines, Watkin and Looney (2018) find that *Dabiq* is unique in utilising images of child perpetrators, giving the "lions of tomorrow" high status, as well as showing they can flourish within the caliphate. Although these three studies research the use of images from different perspectives, they all show that IS attempts to convey important strategic communications from the images within their magazines.

Looking at the research on IS propaganda, some clear inferences can be drawn. First and foremost, the group, via several types of media, deliberately sought to build a brand which was focused on state building, which they achieved using a number of themes. Secondly, the official output by the group was unprecedented in volume compared to any previous group and many scholars have spoken of its sophistication, as well as distinct communications strategies compared to other groups. Thirdly, the group's exceptional output underwent a sizable downturn, both in terms of quantity and quality, and finally, the nascent field of propaganda effects teaches us to be cautious in over-interpreting the sophistication of propaganda as it cannot account for the complex personal and social factors that are involved in engaging with a terrorist organisation.

3.5.4 Twitter

Although IS has always sought to use an array of online media, it quickly became clear that Twitter was the platform of choice for the group. Berger and Morgan (2015) conducted the first "snapshot" of IS on Twitter from September to December 2014. They conservatively estimated that there were 46,000 Twitter accounts in use during this time (their maximum estimate was around 90,000) and the typical user was located within the organisation's territories in Syria or Iraq, as well as other regions in which the group was prominent. They found that 18% of users selected English as their primary language – which is surprising given most of the countries IS was prevalent in were in the Middle East and North Africa, but is an instructive number 'reflecting ISIS's target audience in the United States for inciting and harassing propaganda' (Berger and Morgan 2015, p.14). They find that the average account had 1,000 followers each (far higher than the average Twitter user) and that a relatively small number of "hyperactive" users, tweeting in high volume, account for a large amount of the group's social media output (Berger and

Morgan 2015), not dissimilar to a viral marketing campaign. This is congruous with the research of Fisher (2015), who notes that jihadist groups – including IS – use "swarmcast" tactics; groups developed fluid and dispersed networks to distribute their propaganda online. Rather than central coordination, 'individuals have opted into a loose affiliation as media mujahideen, and actively redistribute content in an attempt to ensure it remains available' (Fisher 2015, p.7). The findings of both Berger and Morgan (2015) and Fisher (2015) point to a bottom-up online strategy in the dissemination of content rather than top-down and centrally planned.

As over 50,000 actors travelled from around the world to join IS in Syria, Iraq, and elsewhere (Cook and Vale 2019), many foreign fighters tweeted about their experience in the caliphate. Carter et al. (2014) followed the social media profiles[5] of 190 Western foreign fighters, finding that Twitter had fundamentally changed the dynamics of jihadist media; they note that the Syrian civil war may be the first conflict in which Western fighters documented their involvement in real-time, including the spreading of battlefield information, links to videos, and official statements. They also highlight the significance of "disseminators", who are not foreign fighters, or even members of organisations like IS, but broadly sympathetic individuals who give moral and political support and are reliable sources of information (Carter et al. 2014). Klausen (2015) analyses the Twitter accounts of 59 foreign fighters in Syria and used a snowball technique to ascertain information about their wider network – totalling around 29,000 accounts, which was then subject to a social network analysis. She corroborates Carter et al.'s (2014) finding regarding the importance of disseminators and also finds that there is a high degree of central coordination behind the social media posts of foreign fighters; not every recruit was allowed to use Twitter and those that did stay on-message and publish at a very high volume, giving the illusion of authenticity (Klausen 2015). This top-down strategy seems to contrast with Berger and Morgan (2015) and Fisher (2015) who posit a bottom-up one. She also highlights the importance of the visual aspect of Twitter, many used pictures on the front line of amenities to express how great life was within the caliphate.

3.5.5 Gender

An important aspect of research into IS is assessing the interplay between gender and the online domain. The idea that female jihadists may have a fundamentally different online experience is not a new one, in 2008, Sageman argued that despite the traditional restriction from females at the forefront of jihadist movements, they were becoming more involved online; 'With the semi-anonymity of the Internet, there is no way of keeping them out. The discussions on certain forums inspire some to want to become more operationally active' (Sageman 2008a, p.112). Similarly, in a YouTube study Bermingham et al. (2009) conducted sentiment and social network analyses, they find a greater support towards AQ from females than males, greater negativity to the outgroup, and importantly, the analyses shows that females held prominent roles within the group.

[5] Both Twitter and Facebook.

When looking at IS, there is support for the idea that the online space may be gendered. Manrique et al. (2016) conduct a social network analysis of IS supporters on Russian platform VKontakte and find, like Bermingham et al. (2009) that, although females are outnumbered, women have superior network connectivity, which can benefit the underlying system's robustness and survival. Using a mixed methods approach, Huey et al. (2017) followed the Twitter accounts of 93 female IS supporters for a year, finding that women fulfil a number of different important roles within the radical online milieu, including: sharing propaganda; recruiting others; posting their experiences from the caliphate; and giving "shoutouts" so those that have been suspended can gather new followers. They find that these roles are vitally important in maintaining social networks and promoting IS ideology, and are both praised and relied on for the success of jihad (Huey et al. 2017). This is also supported by Klausen (2015) who highlights the importance of "Umms" – an honorific title for females – who disseminate content from the caliphate; they note that the top female accounts had a high degree of integration with the most influential foreign fighter accounts. She notes that: 'Online, women are mobilized as partisans and in tactical support roles to an extent far surpassing their involvement in any previous jihadist insurgency' (Klausen 2015, p.16). In Alexander's (2016) case study-based research on female US terrorists, she also highlights the importance of female actors for the dissemination of propaganda on social media.

Analysis of gender is, however, not limited to the study of females. Pearson (2017) analyses the Twitter accounts of 80 IS supporters and discusses the gendered norms within the group. As with the research above, she notes that recruitment may depend on gender; while men may form radical networks in the gym or mosques, for women, social media may be the primary avenue because of their restriction in Salafi circles. She also finds that the online IS-supporting community performs gendered norms; women police each other into fulfilling the role of a female within the movement, while men encourage each other into battle, but the opposite gender is used to shame and police the other into these stereotypical roles (Pearson 2017). Overall, gender is still an understudied topic online (Conway 2016a), and there has been little research on the topic of gender from a male perspective within studies on IS and online extremism, which is a distinct knowledge gap, considering that it is certain that, as Pearson and Winterbotham put it: '[IS] propagates hyper-masculine norms' (Pearson and Winterbotham 2017, p.8).

3.5.6 Jihadi Cool and Low-Level Content

Huey (2015) explores the concept of "Jihadi Cool" on social media, specifically on what she calls "political jamming" – 'the subversion of popular memes to propagate pro-terrorist messages' (Huey 2015, p.1). On social media, Internet "memes" are usually represented as a picture and text which encapsulates a cultural idea or symbol, which is a mode of popular culture among young people today. She finds that IS sympathisers use online images to 'appeal to younger audiences raised within cultures that treat forms of dark, political humour as hip, trendy and counter-culture' (Huey 2015, p.2). Examples range from pictures of world leaders with Hitler, Stalin, Muammar Qaddafi, and Bashir al-

Assad photoshopped in to pictures satirising US military celebrations in Iraq. Importantly, she notes that many young people use social media to develop a sense of themselves and that a key part of this is being "cool", which 'demarcates the boundaries between inside and outside status within social groups' (Huey 2015, p.14). Further evidence of "jihadi cool" can be seen in Huey and Witmer's (2016) study of "IS fangirls", one of the eight groups of women identified in Huey, Inch and Peladeau's (2017) study outlined above. The fangirls, who are between the ages of 15 and 32, post at high volume, attempt to socially manoeuvre and become cool by gaining influential followers. They argue that many of the girls in such networks seem to be more attracted to IS because of their "cool factor" rather than because of ideological affinity; often the content and tone of many posts reflects on the banality of day-to-day life rather than theological discussion (Huey and Witmer 2016).

The concept of "jihadi cool" can be further seen when discussing other types of media introduced by IS and its supporters, such as the production of the video game (or more accurately the production of the trailer), *The Clanging of the Swords*. Al-Rawi (2016) discusses the release of the trailer and the discussion that grew around it on YouTube. The video game appears to be a "third-person shooter", adapted from the popular game *Grant Theft Auto*, with the tagline – 'Your games which are producing from you, we do the same actions in the battlefields [sic]'(Al-Rawi 2016, p.7). Al-Rawi observes that a specific emotional appeal is made to male adolescents who play such games including 'a desire to experience fantasies of power and fame, to explore and master what they perceive as exciting and realistic environments…to work through angry feelings or relieve stress, and as social tools' (Al-Rawi 2016, p.8).

The further "gamification" of jihad can be seen in the propagation of memes which relate to popular games, most famously one which plays on *Call of Duty*, which has a picture of two men, one with a rifle making the religious tawheed gesture with the text "This is Our Call of Duty and We Respawn in Jannah [Heaven]" (Wignell, Tan and O'Halloran 2017; Lakomy 2017b). Dauber et al. (2019) research the use of this *Call of Duty* motif, suggesting that it has strong recruitment potential given two billion people play some kind of video game and the majority of which are in the sweet spot for IS recruitment; younger than 35, male, and technologically savvy. Although the topic of Internet memes and video games may seem quite frivolous at first glance, it is an important and ill-understood aspect of low-level, peer-to-peer interactions that are more light hearted in nature, which is seemingly at odds with the austere and apocalyptic tones in IS' official propaganda (Ingram 2016a).

3.5.7 Online Affordances

While much of the research on IS online focuses on propaganda, a relatively understudied topic is how the Internet is used to instruct or aid terrorist acts. The role of the section of *Rumiyah* called "Just Terror", which is dedicated to instructing attacks, has been discussed above (Reed and Ingram 2017), but there are also other methods that have been utilised. Hughes and Meleagrou-Hitchens, (2017) discuss the role of "virtual

entrepreneurs", a team of around a dozen English-speaking operatives in Raqqa, including British hacker Junaid Hussain. The virtual entrepreneurs would make contact with actors on Twitter who expressed interest in an attack, before moving to end-to-end encrypted apps such as Telegram, where they gave operational advice. Within the US, they played an important role, finding that of the 38 IS-inspired plots from March 1 2014-March 1 2017, 21% involved communication with such an operative, noting that this mode of communication offers a very favourable cost/benefit balance because they require so few resources (Hughes and Meleagrou-Hitchens 2017). Alexander and Clifford (2019) analyse the group's cyber-crime capability, looking specifically at their ability to hack and dox. They note that the group has released a number of "kill lists", identified personal details of government employees and those serving in the military, released via Twitter and other platforms. They find that the group lacks sophistication and there are few instances of people acting on them by targeting those individuals in an attack, however, 'these methods can effectively intimidate the public, cause reputational damage, and ignite fears about the threats posed by terrorism and cyberterrorism' (Alexander and Clifford 2019 p.26).

3.5.8 Other Platforms

During IS' heyday on social media, the focus of the majority of research was on Twitter, which left a sizable gap in knowledge with regards to other platforms. The above-mentioned research by Carter et al. (2014) tracked both Facebook and Twitter accounts, and several studies anecdotally mention the exploitation of other sites by IS – for example, Facebook (Vidino and Hughes 2015; Schmid 2015; Hegghammer and Nesser 2015), and YouTube (Hoyle et al. 2015; Nanninga 2019; Fisher 2015), as well as a number of other platforms such as 'Ask.fm… Instagram, WhatsApp, PalTalk, kik, viper, JustPaste.it, and Tumblr…[and] Encryption software like TOR' (Klausen 2015, p.1). However, there were no studies that specifically analysed IS' exploitation of other sites during their online rise to prominence – this has been somewhat rectified in recent years, which will be discussed below. Conway (2016a) notes that this discrepancy is problematic:

> In the case of violent online extremism research, [there has been] a recent further narrowing of focus to Twitter because of its particular affordances (e.g., ease of data collection due to its publicness) and thus introducing…sample selection bias (Conway 2016a, p.12)

Conway is referring to the "open" nature of Twitter, in which any user can potentially see the post of any other user, making it easier to conduct research than on semi-open platforms like Facebook in which a user has greater control of who sees their content, or closed, peer-to-peer platforms such as WhatsApp, in which research is almost impossible. This creates a knowledge gap which should not be underestimated – the literature has a lot to say about IS on Twitter, but the tactics used by the group and its supporters on other platforms may differ in important ways. That being said, this knowledge gap has lessened more recently.

3.5.9 IS Online Post 2016

Just as the group took substantial physical damage as it lost the battles in Syria and Iraq, a number of regulatory changes across social media platforms, but particularly on Twitter, saw the degradation of IS online. Berger followed up the *ISIS Twitter Census* (Berger and Morgan 2015) with a study a year later which found that suspensions had halted the size and reach of the social network of IS supporters on Twitter and devastated suspended users' ability to maintain followers (Berger and Perez 2016). While the previous study estimated between 46,000-70,000 IS-supporting accounts, he found a year later that fewer than 1,000 English-speaking accounts were readily discoverable and there were fewer than 3,000 in total. These networks had become extremely insular and mostly just communicated with each other (Berger and Perez 2016).

In a similar study on Twitter, Conway et al. (2017) find that accounts of IS sympathisers did not remain online for long; 65% were suspended within 70 days, which caused users to undertake counter-measures such as: making their accounts private, changing to a non-identifying profile picture, and adopting long alphanumeric handles to avoid detection. This is similar to the findings of Alexander (2017), who finds that suspensions have hindered supporters' ability to flourish on the platform and that most accounts last fewer than 50 days and accounts had far fewer followers than previously. Grinnell, Macdonald and Mair (2017), who research the release of the fifteenth issue of *Dabiq* on Twitter, also find that suspensions drastically limit IS supporting accounts' ability to maintain a presence on the platform and that the accounts which were suspended in their dataset were young and had few followers. Similar findings were made in a study on the dissemination of *Rumiyah* on Twitter, too (Grinnell et al. 2018).

As the mainstream platforms became less hospitable for IS, many scholars noted that sympathisers took steps to maintain a presence online. The most notable example of this is migrating to other platforms, particularly to Telegram. Prucha (2016) notes that in early 2016, because of Twitter's robust suspension policy, there was a widespread migration of supporters from the platform to Telegram – a cloud-based instant messaging service which offers end-to-end encryption. He notes that supporters set up hundreds of "channels" and it was normal to create more than 30,000 messages per week, including sharing official content from the group (Prucha 2016). Bloom, Tiflati and Horgan (2017) draw on the importance of the distinction between Telegram "channels" which involve a one-way dissemination of event from the owner, and "chat rooms" which involve interactive discussion. The former, as suggested by Prucha (2016), involve the dissemination of official content, such as photos, recruitment content, beheading videos, audio files, and out links, while the latter are far more informal and contain emojis, "stickers", gifs, and memes. They also note that the move to Telegram highlights the technical innovation of IS supporters as other platforms became more hostile towards them (Bloom, Tiflati and Horgan 2017). In their study of 636 pro-IS, English-speaking Telegram channels Clifford and Powell (2019) note that the move to Telegram comes with a substantial trade-off; the operational security that end-to-end encryption offers

means that their ability to reach potential new recruits is diminished. They observe that the majority of their sample is in private groups or channels which are only available via invitations from URL links (Clifford and Powell 2019).

The move away from mainstream platforms has been more widespread than merely to Telegram. In the above-mentioned study by Conway et al. (2017) on the group's degradation on Twitter, they found 39 different third party platforms which were linked to on the site, six of which, remained prominent over the data collection periods: justpaste.it, IS' server, archive.org, sendvid.com, YouTube, and Google Drive. Interestingly, they found only a very small number which linked to Telegram (0.04%), perhaps because it would mean a lack of control as to who could join via the link (Conway et al. 2017). In a follow-up study to the research on the dissemination of *Rumiyah*, Macdonald et al. (2019) track the out links on Twitter, finding that IS' primary tactic was to use the site to post links to small, file-sharing platforms such as justpaste.it. The notion of intra-platform sharing is also a finding of Weirman and Alexander (2018) who study 240,158 out links on Twitter from 2016-2017, finding that links towards file-hosting sites are utilised as part of IS' apparatus of communications. Shehabat and Mitew (2018) look specifically at IS' exploitation of three file-hosting sites – sendvid.com, justpaste.it, and dump.to – finding them instrumental because they offer anonymity and the upload of content which is easy to distribute. These types of platforms, they argue, have 'allowed ISIS to maintain its flow of information, enlist new actors, and leverage its distributed affiliate and sympathizer networks to reach and mobilize potential jihadists around the world' (Shehabat and Mitew 2018, p.97).

Using mainstream platforms in a coordinated manner is also a finding of a study by Fisher, Prucha, and Winterbotham (2019), who note that IS use multiple platforms in an attempt to avoid detection or suspension. Large platforms such as Facebook, Twitter, and Telegram are "beacons", which direct users to material on "content stores", such as archive.org and YouTube. Finally, "aggregators" collect a range of links to different materials around the web and store them on Facebook pages or websites. Importantly, their findings suggest that 'Despite claims to the contrary, jihadist content is widely accessible via mainstream social media and the surface web' (Fisher et al. 2019, p.2). This claim has been corroborated in studies recently. In a report analysing IS activity on Facebook, Waters and Postings (2018) find that supportive accounts were widespread on the site and that only 43% were removed in the six-month data collection period. Their research also supports the findings of Fisher, Prucha and Winterbotham (2019) in locating propaganda accounts which contained out links to smaller platforms – i.e. the accounts were "beacons". Furthermore, they find that Facebook's "Recommended Friends" function had actively connected at least two supporters within the sample, and it could potentially have had a greater effect (Waters and Postings 2018). In research analysing YouTube's counter-messaging campaign; the "Redirect Method", the Counter Extremism Project (2018) find that, despite the platform's efforts, terrorist material, including videos that showed violence and gore, vastly outweighed the number of counter-message videos. IS attempting to maintain a presence on the largest sites is no

coincidence, many scholars have found qualitative evidence of sympathisers speaking about the virtues of being able to reach larger audiences, particularly when compared to their small reach on platforms such as Telegram (Berger and Perez 2016; Clifford and Powell 2019; Prucha 2016).

Just as with research into the official propaganda, a clear two-stage trend can be ascertained into IS' use of the Internet. In the period leading up to the end of 2015, the group was able to exploit several different social media platforms, particularly Twitter. From around the beginning of 2016, a hostile online ecosystem led to a more pragmatic use of different online platforms to spread their message. Interestingly, the first and second stage roughly align with the rise and fall of the quality and quantity of IS propaganda, leaving the possibility that they are connected. As well as highlighting these two stages, the literature presented in this section suggests a number of other important themes, such as the Internet offering an important space for female supporters, particularly in the dissemination of propaganda. Furthermore, as well as official propaganda, low-level content such as memes and video game motifs could play an important role in the online socialisation of IS supporters. The Internet was also used by IS to provide operational support and to commit cybercrimes such as hacking and doxing. Since the online ecosystem has become more hostile to IS, supporters online have adapted to use different and more complex methods to maintain an online presence. This includes, but is not limited to, a migration to Telegram. Despite this, research shows that they have not fully moved away from the mainstream platforms.

3.6 Conclusion: Locating the Gaps and Research Questions

The overview presented in this chapter offers an opportunity to identify avenues for fruitful research from which the research questions are drawn. To begin, as suggested by von Behr et al. (2013), empirical research which analyses the "supply" of content still greatly outweighs studies that seek to understand how terrorists or extremists actually use the Internet. The growing number of studies in recent years suggest that this is in the process of being redressed, but there is still so much that is not understood and therefore conclusions can only be taken as tentative. In their literature review on online radicalisation, Meleagrou-Hitchens and Kaderbhai (2017) note that the 'use of empirical evidence to draw convincing conclusions remains scarce, and this has greatly impacted on the strength of research on this topic' (Meleagrou-Hitchens and Kaderbhai 2017, p.17). Because of this, there is a need to better understand how terrorists' use the Internet. As noted above, theory has often rested on how content affects users (which is largely unproven). Instead, there is considerable scope, as Ducol (2015) suggests, to reverse the question and instead of asking "what does the Internet do to people?", assess what people do with the Internet. This is the ethos of the empirical enquiry that follows. This is not to say that the supply of content is irrelevant, but rather than objective is to better understand how individuals in this sample of terrorists engage with it.

This chapter has demonstrated that previous research points towards terrorists' utilising the Internet heavily as part of their plots (For example: Gill 2016; Bastug, Douai, and Akca 2018; von Behr et al. 2013). Moreover, studies also tend to suggest that it has become more prominent in recent years (Gill et al. 2017; Jensen, James et al; 2018). Looking at the supply-side, studies which have looked at IS online suggest that the group had both a sophisticated (Winter 2015b; Zelin 2015; Ingram 2015; Pelletier et al. 2016) and wide-reaching (Carter et al. 2014; Fisher 2015; Klausen 2015; Berger & Morgan 2015) propaganda campaign. IS's activities online encompassed a range of different media and objectives. Therefore, the first research question will investigate:

RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?

The existing literature will be drawn from to create quantitative variables to code for different online behaviours. This will include how individuals behave as part of an online network, how they plan for events, and the types of social media they use. These results can compared, where possible, against baseline rates of individuals in the US, as well as against other database studies to demonstrate whether this group of spatially and temporally-specific terrorists are in keeping with other studies on the same topic.

Despite near-universal agreement that terrorists use the Internet as part of their plot, it is less clear whether this has come at the expense of offline interactions. Scholars have previously suggested that this may be the case (Sageman 2008a; 2008b; Weimann 2012; Post McGinnis, and Moody 2014, Anti-Defamation League 2014), but the majority of the empirical evidence suggests that offline activity remains key (Von Behr et al. 2013; Hussain and Saltman 2014; El-Said and Barrett 2017; Reynolds & Hafez 2017) and that activities spill over both domains (Gill et al. 2017; Jensen, James et al. 2018 Baugut and Neumann 2019). Therefore, the second research question will ask:

RQ2: Has the online domain replaced the offline one as the primary venue for terrorists' antecedent behaviours?

This will be done by also creating variables for offline behaviours (similar to Gill et al. 2017), which can then be statistically tested against online activity to assess whether one is more frequent than the other, or whether they are related.

One of the key theoretical suppositions of online radicalisation is that acting on the Internet provides a fundamentally different experience to acting offline. For example, theorists suggest that deviant communities may be formed online which provide individuals with both the ideological and operational support to facilitate involvement in terrorism (Weimann and Von Knop 2008; Neumann 2013a; Koehler 2014; Saifudeen 2014; Neo 2016; Ducol et al. 2016). If this is the case, then one might expect noticeable differences between individuals that use the Internet and those that do not. Moreover, research also suggests that individuals with certain characteristics, such as gender (Sageman 2008a; Pearson 2016) or of a young age (Gill and Corner 2015) may be more likely to use the Internet, therefore RQ3 will assess:

RQ3: Do terrorists that use the Internet exhibit different experiences to those that do not?

This will be analysed by coding for a range of demographic and event behaviours to assess whether specific behaviours or attributes are more likely to result in online activity.

Finally, research tends to focus on the range of problematic aspects of the Internet that may lead to security challenges, such as providing high privacy environments for criminogenic environments to form and grow (Bloom, Tiflati, and Horgan 2017; Clifford and Powell 2019), or providing individuals with instructional materials (Conway, Parker, and Looney 2017; Reed and Ingram 2017). However, research findings have challenged whether the Internet facilitates radicalisation, or if instead, it may hinder terrorists and aid security services (Jensen, James et al. 2018; Gill and Corner 2015). This is particularly important given the high policy priority that has been given to removing as much terror content from the Internet as possible, as discussed in the introduction. Therefore:

RQ4: Does acting on the Internet help or hinder terrorists?

To ascertain this, a number of variables will be included to assess whether an event has been successful which will be tested against different online activities.

As will be expanded upon in the following chapter, these deductive research questions will only drive the research agenda for Chapter 5. For Chapter 6, an inductive methodology based on Grounded Theory will be used which seeks to identify the themes in the data based on the overarching research objective of better understanding online radicalisation.

Chapter 4: Methodology

4.1 Introduction

The previous chapter discussed the concept of online radicalisation, drawing from existing theories and empirical literature to derive four deductive research questions. This chapter outlines how the overall research objective – better understanding the phenomenon of online radicalisation in contemporary terrorism plots – will be empirically analysed using a mixed methods approach. Below, the overall design of the research is articulated; followed by the methods employed to collect data; the inclusion and exclusion criteria applied; the rationale behind the codebook; the analytic strategy; before a short section outlining ethical considerations.

4.2 Research Design

The objective of this thesis is to draw from an empirical dataset of contemporary terrorists to better understand the phenomenon of online radicalisation. As noted in Chapters 2 and 3, it will investigate the behaviours of terrorists, utilising the following working definition of radicalisation: *the process of engaging in terrorism or violent extremist actions.* In essence, the approach will be, as Ducol (2015) advocates: rather than asking what the Internet does to people, it will explore how people use the Internet. This will be done by creating a database of case files of terrorists within the US that acted on behalf IS – including those that successfully conducted attacks, those that travelled to the caliphate, and individuals that were apprehended and arrested prior to their event. These case files will then be analysed using a mixed methods approach, drawing from both deductive and inductive methodologies, to better understand how individuals use the Internet in their pathways towards their eventual activities.

After taking a demographic "snapshot" of the data, the quantitative and (mostly) deductive analysis in Chapter 5 will ask the following research questions:

> *RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?*
>
> *RQ2: Has the online domain replaced the offline one as the primary venue for terrorists' antecedent behaviours?*
>
> *RQ3: Do terrorists that act online demonstrate a different experience to those that do not?*
>
> *RQ4: Does acting on the Internet help or hinder terrorists?*

In answering these questions, the results will be compared to similar studies in the field. Most notably, it replicates many of the coding variables that are used by Gill and colleagues (Gill et al. 2017; Gill and Corner 2015). This will help to contribute to the existing knowledge-base because there are still few data-driven studies which seek to

disaggregate the behaviours associated with online radicalisation. Therefore, it can be fruitful to compare existing findings that research terrorists in a different space and time against this sample. However, other variables are also included if they have been identified as pertinent in the academic literature – an example of this is the inclusion of a variable for the use of end-to-end encryption.

This will be followed by an inductive analysis in Chapter 6, which will draw from a methodology inspired by Grounded Theory, which rather than relying solely on what has been researched previously, this methodology lets the data "speak for themselves", creating hypotheses for future research (Glaser and Strauss 1967).

4.3 Data Collection

To begin, a directory of IS terrorist actors' names was created to identified individuals that operated within the US between the years 2012-2018. Data are collected in three different ways: Firstly, those that have been charged with crimes within the US Criminal Justice System; secondly, those that have been identified as successful travellers to IS territory by Meleagrou-Hitchens et al. (2018); and finally, those that have conducted successful attacks within the US. All the data are collected via open-source methods. This includes court documents such as criminal complaints and transcripts; Department of Justice (DoJ) and FBI press releases; government reports; academic scholarship; news reporting; and online databases.

4.3.1 Criminal Justice System

The first avenue of data collection is actors that have been charged within the US criminal justice system identified via George Washington University's Program on Extremism's (PoE) "ISIS in America" repository, which contains 'over 20,000 pages of criminal complaints, indictments, affidavits and courtroom transcripts detailing Islamic State-related legal proceedings' (Program on Extremism 2019a) pertaining to 166 cases.[6] After identifying the actors to create a directory, the documents were read line-by-line and coded (as described below). These cases provide, by far, the richest data source available, often detailing specific antecedent online and offline behaviours. After collecting data via the PoE repository, a search for the actor's name was conducted on the DoJ website for press releases pertaining to the crime. Then, a literature search was conducted to identify academic scholarship in which the actor has been mentioned. The actor's name was then cross-referenced against other online terrorism and extremism databases such as the Counter-Extremism Project (Counter-Extremism Project nd) and the Investigative Project on Terrorism (Investigative Project on Terrorism nd) – the latter of which yielded a number of court documents that were not included in the PoE repository. Finally, the actor's name was run through searches on Lexisnexis and Google News to collect journalistic sources. While not as rich as the PoE data, journalistic sources often provide a very detailed account of actors' early lives and utilised primary data such as interviews

[6] As of the end of data collection on 31st December 2018.

with friends and family members. As of the end of data collection on December 31, 2018, the PoE repository had 166 different cases.

4.3.2 Travellers

The second avenue of data collection is documenting the actors who were identified as having travelled to IS abroad. This provided several challenges. Firstly, there is not an official list of those that have travelled to join IS. In 2017, the FBI noted that there were 250-300 US jihadists that had travelled or attempted to travel to Iraq and Syria (Interview with FBI agent, quoted in: Meleagrou-Hitchens et al. 2018), but this figure is an approximation and represents more than those that travelled to join IS. Meleagrou-Hitchens et al note that 'this number includes travelers, attempted travelers, and participants of jihadist and non-jihadist groups' (Meleagrou-Hitchens et al. 2018, p.87). Given that many of those that have been charged are would-be travellers, this lowers the number significantly. Furthermore, the mobilisation of foreign fighters to several different jihadist groups, particularly Jabhat as Nusra (Nusra Front), and non-jihadist groups such as the Free Syrian Army, creates doubt as to the total number. The second challenge pertains to data; many of the successful travellers have not been formally charged and, as such, the richest data source – court documents – is not available. The third, and an interrelated, challenge is that travelling to a foreign conflict is not as newsworthy as plotting an act of domestic terrorism and there is a noticeable drop-off in the richness of the journalistic data for some actors.

Despite these limitations, collecting data on this population is a fruitful endeavour. In their report, *The Travelers*, Meleagrou-Hitchens et al. (2018) identify 64 successful travellers, and have later increased their number to 72[7] (Program on Extremism 2019b).[8] Furthermore, a small number of the travellers *have* been charged by the US criminal justice system and a number have details of their plots explained in the court documents of others. An example of this is Yusuf Jama, who died less than a year after arriving in Syria and was never charged, but important details of his case are laid out in the criminal complaints of Guled Ali Omar[9] and Abdirizak Warsame.[10] The report by Meleagrou-Hitchens et al. (2018) is the most reliable source of identified travellers and as such, was used to create the second directory. Data were collected firstly via a literature search, then via cross-referencing against the online databases, then via Lexisnexis and Google News, as outlined above.

[7] As of December 31st 2018.

[8] These 64 include those that have travelled to join IS, AQ affiliates, and other jihadist groups, but excludes other mobilised groups such as the Free Syrian Army.

[9] USA v. Mohamed Abdihamid Farah et al, Criminal Complaint, Case 0:15-cr-00049, United States District Court for the District of Minnesota, 2015.

[10] USA v. Abdirizak Warsame, Criminal Complaint, Case 0:15-mj-00978-HB, United States District Court for the District of Minnesota, 2015

4.3.3 Attackers

The third data source is compiled by identifying the successful incidents of terrorism on the Global Terrorism Database (GTD) (START nd). Because the categorisation system for the GTD takes a conservative approach to labelling groups, searching for IS within the US does not yield any responses. Therefore, a search was conducted for all incidents of terrorism within the US (for a wide date range of 2005-2018) using the first (and widest) criterion for a definition of terrorism (The act must be aimed at attaining a political, economic, religious, or social goal). The search returned 365 responses and each case was assessed using the inclusion and exclusion criteria laid out below. Note that the GTD is a database for terrorist incidents, not individual actors. Therefore, when an incident involved more than one actor, each were individually tested against the criteria and, if met, a distinct case file was created for each. An example of this is the attack in San Bernardino on December 2, 2015, by Rizwan Farook and Tashfeen Malik,[11] who have one entry on the GTD, but are treated as separate entries in this research.

After the directory was created, data were collected in a similar way, via a literature search, cross-referencing against online databases, and a search of Lexisnexis and Google News. Given the high-profile nature of many of these attacks, the data for these actors proved to be very rich. There was a high degree of crossover between those that have been charged in the US and the result of this search. Furthermore, there were often cases of actors being charged that provided detailed accounts of the successful attacks of others. An example of this is Noor Zahi Salman,[12] the wife of the Pulse nightclub shooter, Omar Mateen.

Overall, there are 166 cases identified in the PoE repository, 72 cases identified by Meleagrou-Hitchens et al. (2018), and 365 incidents returned on the GTD. For a total of 603 cases to assess against the inclusion and exclusion criteria – laid out below. After doing so, and accounting for duplicates,[13] the final sample size is 201 actors. A flowchart demonstrating this process can be seen in Figure 5.

4.4 Inclusion and Exclusion Criteria

This database is a collection of "Islamic State terrorist actors in the US" which ranges from 2012-2018, and as such, there are several clarifications that must be made to elucidate exactly what constitutes being included in the sample. Firstly, it is important to establish

[11] Megan Christie et al., Christmas Party May Have Triggered San Bernardino Terror Attack: Police, *ABC News*, December 1, 2016, Available at: https://abcnews.go.com/US/christmas-party-triggered-san-bernardino-terror-attack-police/story?id=43884973.

[12] Salman was eventually removed from the database because there is insufficient evidence that she fit the inclusion criteria. However, the richness of the data regarding Omar Mateen within her criminal justice files vindicates the decision to collect as much data as possible, before then acting on inclusion and exclusion criteria.

[13] There is overlap between the three sources of data. For example, Abdi Nur and Mohamed Roble were charged, appearing in the PoE repository and were named in *The Travelers* report. Similarly, Edward Archer conducted a successful attack, appearing in the GTD, but was also charged and therefore appeared in the PoE repository.

what being part of IS entails; membership of contemporary terrorist organisations is often more fluid than in past decades. Secondly, the issue of what constitutes "being a terrorist" offers several problems, as outlined in Chapter 2. Thirdly, it must be established what is sufficient to deem the actor or action being "in the US". Finally, several cases are excluded on the basis of a dearth of data, for which the criteria are laid out below.

4.4.1 Islamic State

Membership of a terrorist organisation has fundamentally changed in recent decades. While the debate of "old" vs "new" terrorism has never been satisfactorily settled (Crenshaw 2007; Macdonald and Mair 2015), for many organisations, particularly jihadist ones, the notion of a "formal member" does not accurately represent the group dynamics. Rather, smaller cells of individuals conduct attacks that are inspired by a group (Sageman 2008a). In the case of IS, now-deceased Abu Mohammed al-Adnani, the group's official spokesman gave a speech on 22nd September 2014 in which he instructed supporters to plan attacks in their own country if they could not travel to IS territory (Shane 2016b; Vidino et al. 2017), which was echoed in the group's propaganda (Reed and Ingram 2017). This type of IS-inspired attack has been described as "the new normal" by then-FBI Director James Comey (Susman 2015), while Europol observe that 'Jihadist actors can be both directed by IS or merely inspired by IS ideology and rhetoric' (Europol 2017, p.5). As such, only including actors based on being active members of the central organisation will not reflect the reality of the sample.

As a solution, I follow the National Consortium for the Study of Terrorism and Responses to Terrorism's (START) lead of group membership inclusion for their "Profiles of Individual Radicalization in the United States" (PIRUS) Codebook:

> We define "member" broadly. This includes official members, individuals in the US government or another government claimed were members…and includes credible media sources link to the group (but not those based on pure speculation). It also includes individuals who claim membership…even if the group itself does not acknowledge membership (START 2018, p.6)

This criterion allows for self-identification to a terrorist group. The next question is how one can identify and code behaviours pertaining to self-identification. There are two ways in which one can be judged to self-identify:

1. Outward: Words or actions that display support for the group such as publicly stating it (online or offline) or attempting to recruit others.
2. Inward: Activities such as downloading, reading, or listening to the group's or sympathisers' media content.

Importantly, this *must* be accompanied by actions for which self-identification can be ascribed a significant role. Again, the PIRUS Codebook is instructive: 'where it appears from the open sources that ideological motives were the prime driver of the decision to engage in illegal behavior' (START 2018, p.3). It should be noted that an actor can identify

with multiple groups (for example IS and AQ), but it is necessary that they display inward or outward self-identification with IS.

A further ambiguity is the relationship of the Nusra Front to IS, and the relationship of AQ to each of them. In October 2004, under the lead of Abu Musab al Zarqawi, the precursor group to IS swore allegiance to AQ and became al Qaeda in Iraq (AQI), which lasted officially until 2013, although the relationship had soured as early as 2006 (Whiteside 2016). As the group expanded at the beginning of the 2010s, and the Syrian Civil War broke out, IS Emir Abu Bakr al-Baghdadi sent a group of fighters, including Abu Mohammed al-Julani, who was a high-ranking member of IS, to set up what became the Nusra Front (Turner 2015). On April 8th, 2013, Baghdadi unilaterally announced that the Nusra Front was part of IS, which was rejected by both Julani and AQ's leadership, causing a series of arguments and occasionally open fighting between IS and Nusra Front, resulting in an eventual split between the groups (Stern and Berger 2015). As such, there is a degree of conceptual confusion as to whether Nusra Front was ever part of IS as the split occurred before it existed in its current form. Given that the two groups have become distinct entities in the years that followed this split, it is prudent to understand them as different groups, even if they share a common ancestry. As such, those that were members or self-identified as members of Nusra Front, and for which there is no evidence of membership or self-identification with IS, are not included.

4.4.2 United States Definition of Terrorism

Terrorism studies has long grappled with the debate surrounding the wide array of different definitions of terrorism (Ganor 2002) with many claiming that it fulfils the interests of power holders who have "defining agency" (Schmid 2004). Adopting the US judicial definition is intuitive for a dataset comprised of actors in the United States, particularly because the main avenue for data collection come from cases with criminal charges. However, there are several problems that arise from using the United States judicial and legislative definitions of terrorism.

The US is unlike many other countries in that it distinguishes between acts of domestic and international terrorism (Hardy and Williams 2011). Title 18, §2331 defines "international terrorism" as activities that:

a) Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
b) appear to be intended—
    i. to intimidate or coerce a civilian population;
    ii. to influence the policy of a government by intimidation or coercion; or
    iii. to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
c) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are

> accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. (18 U.S.C. §2331, 2001)

While "domestic terrorism", which was introduced by the USA PATRIOT Act in the weeks after the events of September 11th 2001, is defined as activities that:

a) Involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State
b) Appear to be intended:
    i. to intimidate or coerce a civilian population;
    ii. to influence the policy of a government by intimidation or coercion; or
    iii. to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
c) Occur primarily within the territorial jurisdiction of the United States. (18 U.S.C. §2331, 2001)

Hardy and Williams argue that these definitions, like many democracies' definitions of terrorism, are too broad and have historically 'been used to target, detain and prosecute individuals with no real connection to terrorism' (Hardy and Williams 2011, p.156). They also highlight the large number of "Federal Crimes of Terrorism" that have created disagreement amongst federal agencies in which activities should be regarded as terrorism (Hardy and Williams 2011).

Furthermore, groups may be designated as foreign terrorist organisations (FTOs) by the US Department of State, of which the precursor group to IS was added on December 17, 2004 (US State Department nd). There is no such list for domestic groups (Zakaria 2018). The importance of these designated groups stems from 18 U.S.C. §2339B, which criminalises providing material support or resources to a designated FTO (18 U.S.C. §2339B, 2015). Despite there being no equivalent for domestic groups, there remains a non-defined group charge for providing material support or resources to an offense identified as a federal crime of terrorism (18. U.S.C. §2338A, 2009). This is important for the coding of this research because, like the 18 U.S.C. §2331 definition of terrorism, the material support charge has been interpreted broadly when prosecuting, including:

> Property, services, money, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, and transportation (Berkell 2017, p.283)

Berkell also notes that the statute includes both an "attempt to provide material support" and "conspiracy to provide material support" charge, which enhance the pre-emptive power and mostly hold the same penalties as the substantive charge (Berkell 2017). This includes travelling and attempting to travel to join a foreign terrorist group, as "personnel" is interpreted to include oneself in the form of travel (Meleagrou-Hitchens et al. 2018).

4.4.3 Other Crimes and Terror Enhancements

To make matters more complicated, despite the US definition and statutes surrounding terrorism being often described as broad, including only those charged with terror offences is also too narrow to accurately describe the data. Rather, in many situations, actors are charged with non-terror related crimes – often either making false statements to the FBI or felon-related gun charges. If a guilty plea or conviction is secured, then a "terrorism enhancement" can be (but is not always) added at sentencing:

> The enhancement…applies in two scenarios: one, where the sentencing court finds that the defendant's offense "involved" or was "intended to promote" a federal crime of terrorism; or two, where the court finds the offense was "calculated to influence or affect the conduct of government by intimidation or coercion," even if there was no "federal crime of terrorism" (Skinner 2015, pp.334–335).

For coding this data there are two problems with the terror enhancement. Firstly, at the end of data collection in December 2018, many of the cases are still ongoing and therefore it is unknown whether a judge would utilise the terror enhancement at sentencing. Secondly, the enhancement is subject to prosecutors making plea deals with defendants. Judges are not compelled to obey such deals, but they often do. As such, a case that would otherwise have had a terror enhancement may not for discretionary reasons.

Not charging an actor with a terrorism-related crime is, in practice, often due to reasons of expediency rather than a judgement of whether the crime constitutes terrorism. Most returnees from Iraq and Syria have not been charged with material support, but rather lying to the FBI as the evidentiary bar is high and access to evidence is low:

> In order to conclusively prove any material support charge, or the terrorism enhancement to false statements charges, prosecutors must provide substantial evidence that the traveler in question had connections to a designated foreign terrorist organization. The built-in defense for travelers is that although they may have provided support to a militant organization in Syria or Iraq, they did not support a designated organization (Meleagrou-Hitchens et al. 2018, p.77)

In other words, there is a calculated cost/benefit analysis based on how likely prosecutors believe they are to successfully secure a conviction or a guilty plea.

It should be clear that merely defining a terrorist as one that has been charged with terror offences or one that has a terror enhancement at sentencing is problematic for several reasons. Firstly, the definition of those that are charged with terror offences may be too broad, given, as Hardy and Williams (2011) argue, many of these individuals have no connection to terrorism. Secondly, it may also be too narrow because the practicalities of prosecuting terrorists do not always yield a terror-related charge or enhancement. Thirdly, those formally charged do not represent the whole sample. Many of the successful travellers and successful attackers have never been charged with any offence – often because they died before the security services were aware of them.

4.4.4 Other Definitions of Terrorism

Despite the above-mentioned issues with the US's approach to designating and prosecuting terrorism, this represents a wider problem of attempting to define an essentially contested concept (Gallie 1955). However, the absence of a universal definition of terrorism does not imply that the term is devoid of meaning (Meserole and Byman 2019). Scholars have suggested that there are core components to understand the term. Phillips (2015) notes that there are three key elements in widely accepted definitions: (a) intentional violence; (b) that the violence is used to spread fear in a wider audience; and (c) political motivation. Both the international and domestic US definition hit these core components – violence (or threat); coercion via terror; and towards an ideological goal.

To make matters slightly easier, this research is concerned with individuals that self-identify as part of a group for whom there is no doubt are a terrorist organisation. Not only do they appear on the State Department's list of FTOs, but they are also the subject of UN Security Council in Resolution 2253 (United Nations Security Council 2015), which encouraged member states to designate the group at the national level. The group has been proscribed by the United Kingdom, the US, France, Australia, Canada, and the European Union (Terrorism Content Analytics Platform nd). Given that the first inclusion criteria required affirmative evidence that the individuals self-identify with the group and then acted with clear ideological motivation, this means that the "edge cases" will have already been removed because all actors charged with terror-related crimes and those given terror enhancements are included if they have met the self-identification criterion. An example of this process is the cases of Mohommad Ali and Sumaiya Ali, a married couple who lied about their sons'[14] whereabouts. Given the available evidence, they do not meet the first criterion of self-identification and as such are removed despite being charged with a terror-related offence.

The more difficult task is judging those that were neither charged with a terror-related offence nor were they given a terror enhancement. The most feasible solution is a judgement as to whether it would constitute the US definition of terrorism, based both on an interpretation of the event to the definitions outlined in 18 U.S.C. §2331 as well as other similar cases. For example, it is safe to say that all of the travellers for whom there is evidence that they successfully joined IS can be considered to have committed the crime of Material Support for an FTO, as many other actors have been successfully charged on these grounds. Again, given that the criteria for self-identification and acting on ideological motives, the justification for either a terror-related crime or an enhancement should be relatively clear.

The actor must:

a) Have been charged with a terror-offence, or

[14] Their sons did join the caliphate and are included.

b) Have been sentenced with a terror-enhancement, or
c) Be judged to fulfil the United States definition of terrorism as outlined in 18 U.S.C. §2331 and by comparing similar cases.

4.4.5 United States of America

Further ambiguity is created by the question of what constitutes acting in the United States; whether it is the nationality of the actor, or residence status, where the plot was planned, or where it was due to take place. For their PIRUS codebook, START use the following criterion: 'the radicalization process must have begun and significantly advanced within the US…This is to be distinguished from individuals who were radicalized in a place other than the US' (START 2018, p.5). I judge this to be too narrow to accurately portray the data in this project. Given the international nature of IS – with territory in several countries and committing attacks in others – it makes little sense to exclude cases which may, for example, have been planned in, and targeted the US by a citizen, but had begun their trajectory abroad. On the other hand, it also makes little sense to include US citizens if they have not been in the country for several years – actors may have left the country before IS or its precursor groups had been established. The important aspect is that the US must play a significant role. I chose to judge this iteratively having collected all the data; feeling that five years best represents a reasonable cut off point to consider the US being significant in their activity. This, for the most part, allows for the timeframe which includes IS' rise to global prominence.[15] An example of an excluded case is Ahmad Abousamra, who fled the US in December 2006, but as Meleagrou-Hitchens et al. (2018) note, it is unclear what he did between that time and the first verification of him joining IS in 2014.

Firstly, all those charged in the US with crimes pertaining to their activity are included – this is already covered in the criteria above. Secondly, US citizens are clearly "Americans" and should also be included, but only if they have been living in the country at some point in the five years before their event. Thirdly, those who have been granted permanent residence or resided in the US at the time of their event are also included (in the case of those travelling to IS, the event is leaving the US).

The actor must:

a) Have been charged in the US, or
b) Be a US Citizen, living in the US up to five years before their event, or
c) Be a permanent resident, or
d) Resided in the US at the time of their event.

4.4.6 Dates

Rather than set an arbitrary date range, this research is dictated by the start point of IS activity, as laid out by the data sources, up to the end of data collection on 31st December 2018. The first data source, the PoE repository (the most comprehensive list of those

[15] The median year of arrest/act of terrorism/travel is 2015.

charged with IS-related crimes), suggests that the first event was on November 9 2013.[16] The second data source, the travellers directory, has cases of people travelling to join IS from an unknown time in 2012,[17] while the third data source, collected from the GTD, finds the first applicable attack as being conducted on June 1 2014.[18] It should be noted that these are not inclusion criteria, because this research aims to track every case it does not have a formal start date, but the first reported instance is in 2012.

4.4.7 Exclusion for Insufficient Data

After collection, it was clear that there is a disparity between the richness of data in different cases. In some instances, there is so little information that nothing can be learned about their antecedent or event behaviours. This is most often the case with travellers, such as Mamadou Bah, who is listed in Meleagrou-Hitchens et al.'s (2018) report, but for whom no other information could be gathered. Given that the data are coded in a dichotomous manner ("yes" versus "not enough evidence to code yes") this is likely to lead to over counting of the latter that could skew the results.

Therefore, those for whom no antecedent *and* no event behaviours could be determined – that is to say, nothing about their pathway towards terrorism, and nothing about the act itself – are removed from the sample. It is important not to remove data points on the basis of it not being the dependant variable (Internet usage), so it must be that there is no information regarding online or offline behaviours. There is precedent for this type of exclusion. In their study of online terrorists in the UK, Gill et al. (2015) remove Irish Republican actors from their sample because their online activities were rarely reported in open sources:

> Their inclusion would, therefore, make the data analyses biased to an unacceptable extent as each field would be entered as a 'No', thus dramatically undercounting the likely representation of online behaviours by Irish Republicans (Gill et al. 2015, p.13).

Using open-source data is still likely to undercount the dependant variable to some extent, which is an unavoidable limitation. However, this provides a reason not to skew the data further.

[16] This is the travel of Aws Mohammed Younis al-Jayab: USA v. Aws Mohammed Younis al-Jayab, Criminal Complaint, Case 1:18-cr-00721, United States District Court for the Northern District of Illinois, 2016.
[17] This is the travel of Russel Dennison: Trevor Aaronson, How the FBI Created a Terrorist, *The Intercept*, March 16, 2015. Available at: https://theintercept.com/2015/03/16/howthefbicreatedaterrorist/.
[18] This is the attack of Ali Muhammad Brown. Thomas Moriarty, How Brendan Tevlin's murder case is an example of a new kind of terror, *NJ.com*, May 14, 2019. Available at: https://www.nj.com/essex/2018/04/brendan_tevlin_killing_reflects_terror_threat_expe.html.

Key:
Green = Yes – Move on to next stage
Red = No – Next question in current stage, or if final question, exclude.

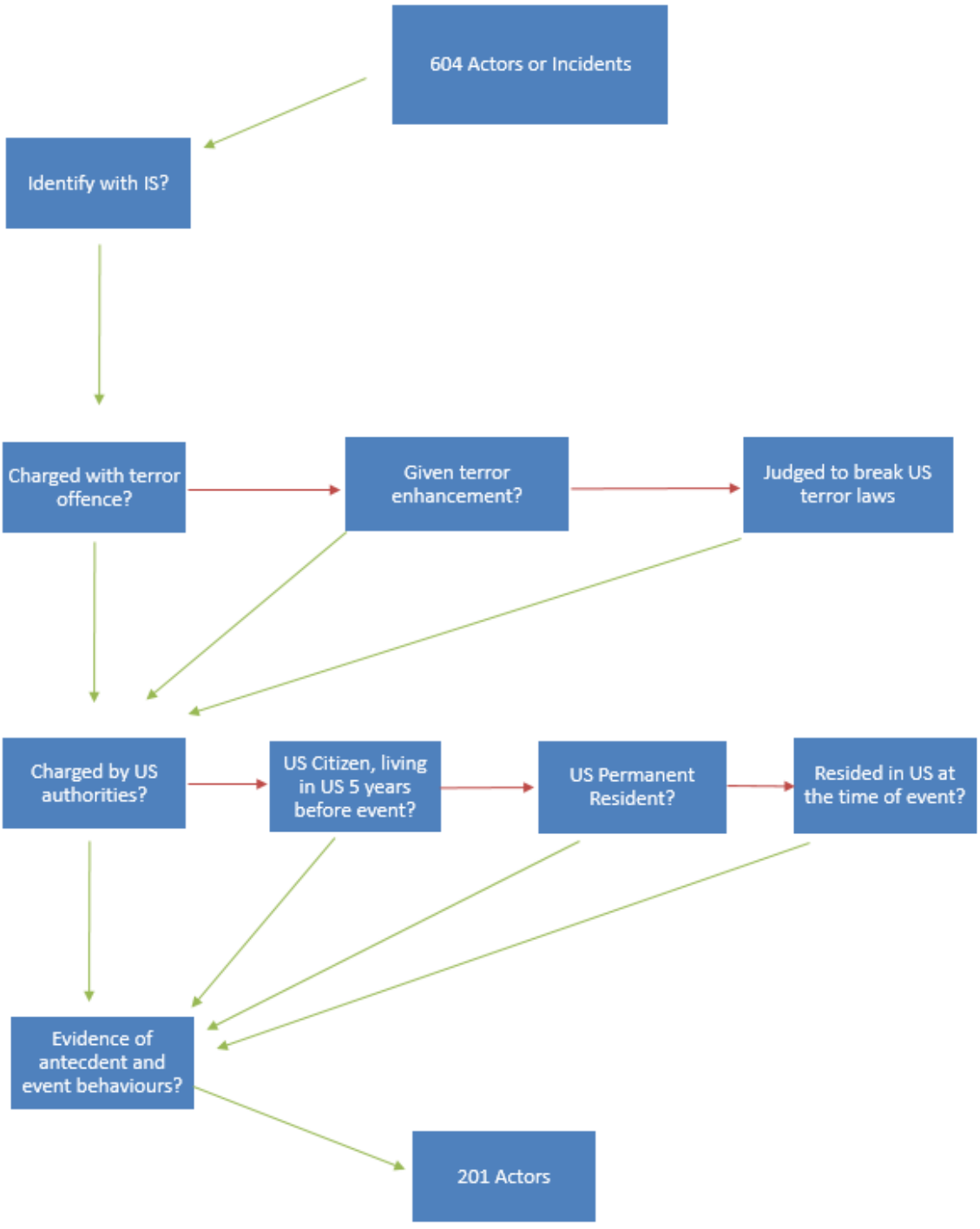


Figure 5 - Flowchart of Inclusion/Exclusion Criteria

4.5 Quantitative Coding

4.5.1 Analytic Rationale

In popular discourse in recent years, the Internet has often become a monocausal explanation for engagement in violent extremism, in both the media (New York Times Editorial Board 2018; Tufekci 2018) and by policymakers at the highest level (Elgot 2017). This research attempts to disaggregate what is often referred to as "online radicalisation" as discrete and identifiable behaviours to answer four research questions:

> *RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?*
>
> *RQ2: Has the online domain replaced the offline one as the primary venue for terrorists' antecedent behaviours?*
>
> *RQ3: Do terrorists that use the Internet display a different experience to those that do not?*
>
> *RQ4: Does acting on the Internet help or hinder terrorists?*

The primary influence for the quantitative analysis is the database studies of Gill and others, that seek, in a similar way, to disaggregate the term (Gill et al. 2017; Gill and Corner 2015; Gill et al. 2015; Gill 2016). In their research on lone actor terrorism, Gill and Corner (2015) split the term into two types of behaviour: engaging virtually with other actors and learning or planning their eventual attack. They then disaggregate each type into further behaviours, such as:

For virtual interactions, using the Internet to:

a) Reinforce prior beliefs,
b) Seeking legitimisation for further actions,
c) Disseminating propaganda,
d) Signalling their intended activities, and
e) Recruiting others.

And for learning or planning their eventual activity:

a) Accessing ideological content,
b) Opting for violence,
c) Choosing a target,
d) Preparing an attack, and
e) Overcoming hurdles (Gill and Corner 2015).

These behaviours are used as variables for several studies both in research on lone actors (Gill 2016) and a combination of lone and group actors (Gill et al. 2017; Gill and Corner 2015; Gill et al. 2015; Gill 2016). Gill and others' research seeks to improve the understanding of online radicalisation in several ways, such as: discerning whether those who interact virtually or learn online display observably different experiences than those

who do not; whether the online space has replaced previous locations in which "radicalisation" occurred; and whether the Internet helps individuals overcome hurdles in their plans (Gill et al. 2015).

This research aims to build on these database studies of convicted actors within the United Kingdom, with a dataset from US-based IS actors. In Gill and others' work, they decide to limit the focus to a single country because different countries may employ substantially different degrees and methods of reporting on terrorist incidents and their use of the Internet (Gill et al. 2015). Given the need for English-language reporting and a sufficient number of cases of terrorism to be statistically significant – both of which are requirements shared in this research – they settle on a choice between the United Kingdom and the US, eventually choosing the UK. As a result, a database which focuses on a sample of US terrorist actors will contribute to the literature and, given the replication of many of the coding variables, provides a valuable means of comparison to the work of Gill and others.

Importantly, this research also takes its lead from Gill and others in collecting and coding a wide range of terrorist actors, rather than those that are purported to have "radicalised" online. If it were to limit itself to that dataset, it would fall foul of the methodological problem of sampling the dependant variable. That is to say:

> If the present study were to simply consider only individuals reported to have been radicalised via the Internet, we would be unable to look at the correlates of terrorists' decisions to use the Internet as the data would not include those cases that neglected to use the Internet (Gill et al. 2015, p.12)

In other words, without looking at the behaviours of those that have not used the Internet, it would not be possible to assess whether the behaviours of those that act online are discernibly different from those that do not act online.

4.5.2 Accounting for Missing Data

When using open-source data for quantitative analyses, there are two different ways in which the researcher can code. Firstly, some studies – including Horgan et al. (2016) and START (2018) – code using three answers: "Yes", "No", and "Not enough information". For example, when attempting to establish whether an individual uses the Internet to disseminate propaganda, a lack of any evidence would be treated in the third category of "Not enough information". The second way is to code the variables in a dichotomous manner – that is to say "Yes" or "Not enough information to code yes". This is used by Gill et al. (2017). In the same example of coding for the dissemination of propaganda, a lack of evidence would be treated the same way as a definitive "No". This thesis utilises the second of the two systems for most variables – the variables with multiple answers (such as type of employment or marital status) do allow for an "Unknown" answer. However, both systems have flaws and considerations that are laid out below.

An important consideration are the differences in assumptions between the two types of coding. The first takes the assumption that incomplete data are missing at random (Safer-Lichtenstein, LaFree, and Loughran 2017) while the latter carries the assumption that missing data are more likely to be negative than positive. The latter system is utilised by Gill et al. (2017) in their study of online behaviours, who justify it on the grounds that most open-source reporting on terrorism does not detail what the individual *did not* do, and as such:

> Definitive "no" answers were a rarity (less than 5%) within the data collection process. This percentage was generally uniform across most variables. Usually these "no" answers only occurred in response to incorrect reporting earlier in the news cycle about a particular offender. (Gill et al. 2017, pp.105-106)

In other words, Gill and others suggest that there are so few cases which confirm a negative that it would present findings heavily skewed against the true representation of these negatives. They note that using multiple imputation methods may be possible if there were more definitive "No" answers in the data, positing that this level of granularity necessitates access to closed-source data such as police records. Although Horgan et al. (2016) use a three-answer system in their open-source behavioural study on US-based terrorists; they make a similar point when discussing limitations:

> While it is universally true in open-source coding that the number of true "YESs" will likely be a truer representation than the number of "NOs" in this dataset it may be especially true for behavioral factors associated with nonillegal activities or terrorist activities that occurred abroad.' (Horgan et al. 2016, p.1236)

That is to say, non-illegal activities are less likely to be reported on and therefore will inflate the "Not enough information" category at the expense of the "No", giving inaccurate findings.

On the other hand, a dichotomous coding system is not without its flaws. All else being equal, it is good practice to minimise assumptions when coding. Safer-Lichtenstein, LaFree, and Loughran (2017) make the point that terrorism studies has not thoroughly considered the reprecussions of assumptions around missing data. They argue that the most reasonable methodological starting point is to ask what can be definitively said about the data without making any assumptions regarding the missing data. They empirically demonstrate that different assumptions can create misleading findings that are not reflected when the assumptions are removed (Safer-Lichtenstein, LaFree, and Loughran 2017). To code using a dichotomous system assumes that data are not missing at random; the arguments offered by Gill et al. (2017) and Horgan et al. (2016) offer a justification for this. However, it means that when using this system, "No" will be overcounted to a non-trivial level. Importantly, Safer-Lichtenstein, LaFree, and Loughran (2017) note that in empirical research within the terrorism studies literature, these assumptions are not explicitly stated and justified, and call on researchers to be more

transparent in future. As such, it is important to dedicate this space to both openly state the assumptions which are being adopted and also justifying the reasoning for it.

Looking back retrospectively having coded the data line-by-line multiple times, taking the decision to code most variables dichotomously is the correct one. The arguments given by Gill et al. (2017) and Horgan et al (2016) regarding the lack of instances in which negatives are confirmed seem to hold true for these data as well. There are some exceptions to this, for example, previous criminal convictions *were* regularly mentioned, even if the individual did not have one. This makes sense given how much of the dataset is made up of court documents, for which this factor is important in bail hearings and sentencing. However, in general, the assumption that missing cases are more likely to be "No" than "Yes" seems a robust one given the quantity and richness of the data relating to the key variables of communicating with co-ideologues and the learning or planning of the actors' eventual activity, suggesting that if variables are present, it seems likely that they would be reported. There are a small number of instances in which this assumption's flaws are apparent, such as the case of Mohimanul Bhuiya, who travelled to Syria without any apparent communication with co-ideologues (online or offline). One may intuit that this is unlikely given the degree of coordination that is usually required to get an individual into the caliphate, and therefore is more likely caused by a lack of data. However, these cases are relatively small in number, and compared to the greater drawback of there being so few cases which confirm a negative, this seems like an acceptable trade-off. However, this research heeds Safer-Lichtenstein, LaFree, and Loughran's (2017) advice by being transparent about these limitations.

4.5.3 Codebook

To answer the four research questions, the data are coded in a two-step iterative process, similar to that laid out by Gill et al. (2015). A codebook was developed from the academic literature and data were collected and coded against it, saving each of the data points electronically. As data were being collected and coded, emergent themes and patterns were turned into variables. This is particularly important given that the first research question seeks to explore the different types of online behaviour. After the first round of data collection, the whole dataset was revisited and coded against the revised codebook. There are four types of data: demographic; network behaviours; event behaviours; and post-event behaviours. Below, the variables are outlined with explanations for why they have been chosen. There are 4 types of variable in this codebook: Firstly, categorical variables relate to a limited number of non-linear labels, for example, mental health diagnoses. Importantly, dichotomous variables – which make up most of this codebook – are a type of categorical variable with only two possible answers; i.e. Yes/Not enough information to code yes. The second type of variable is numeric, such as the age of the actor at the time of their event. Thirdly, string variables are used when a name is appropriate, for instance, the name of social media platforms used, and finally, a date variable is used for the date of the terrorists' event.

Demographic

Several demographic variables were included to offer a snapshot of the dataset. Research has long found jihadist terrorists and foreign fighters in the West to be demographically heterogeneous (Vidino et al. 2017; Klausen 2016a; Hegghammer 2013; Vidino and Hughes 2015). As well as potentially confirming or challenging this consensus, demographic variables can be tested for independence against online behaviours to determine their relationship. On that note, the following demographic variables are created:

Age: Gill et al. (2015) find that younger offenders were significantly more likely to engage in virtual interaction and online learning than older ones.

Gender: Research has consistently found terrorists tend to be predominantly male, both for Islamists (Vidino et al. 2017; Vidino and Hughes 2015; Klausen 2016a; Bryson 2017; Webb 2017) and more generally (Gill et al. 2015). Coding for gender allows for inspection into potentially different processes for male and female IS actors, as has been suggested in other studies (Pearson 2016; Bermingham et al. 2009).

Employment: There has been a long-standing debate as to the relationship between economic factors and terrorism (Piazza 2006; Piazza 2011). Given the difficulty in measuring economic hardship using open sources (Bryson 2017), employment status remains one of the best indicators. Database studies have returned no clear consensus on this, with Sageman (2004) suggesting that underemployment played an important role, while Bakker's (2006) study of European jihadists questions that relationship. Gill et al. (2015) find that one third are unemployed, while Horgan et al. (2016) find only 11.8% to be unemployed. There are two variables, one dichotomous (i.e. was the actor employed at the time of their event?) and one categorical (what kind of occupation did the actor have?)

Family Characteristics: Research has also returned conflicting conclusions regarding family characteristics. Sageman (2004) and Horgan et al. (2016) both find that of those who had marital status information available, the majority were married and had children, while Bakker (2006) finds married, single, and divorced actors to be evenly spread out. This consists of three variables, one categorical variable pertaining to the actors' youth (i.e. were they raised in a dual parent family, single parent family, or other kind of guardianship?), one categorical pertaining to current relationship status, and one dichotomous regarding to whether the actor was a parent.

Country/City/State of Residence: There is a substantial amount of research which points to the importance of what have been deemed "radicalisation hotspots" (Vidino et al. 2017; Varvelli 2016b; Soufan Group 2015). Rather than equal distribution of terrorists or foreign fighters according to Muslim populations, certain areas are accountable for substantially higher levels of recruitment, which is attributed to factors such as charismatic figures or criminogenic environments. This is particularly important in the context of "online radicalisation", as Reynolds and Hafez (2017) suggest, because if the Internet plays a primary role over the offline domain, one might expect a relatively equal

distribution of recruitment. Three string variables are created to denote the country, city, and, if applicable, US state of residence. For cities, the larger metropolitan area is used, for example, New York City rather than Brooklyn or Queens.

Country/City/State of Birth: Similarly to the variables above, coding for states of birth can help identify if there is a clustering within different geographical areas. Furthermore, there is currently a debate involving high-level policymakers in the US surrounding the threat of Muslim immigrants. This variable can offer an insight into the behaviours of those born in the US against those that were not.

Citizenship/Ancestry/Refugee: These three variables will inform the policy debate regarding Muslim immigrants and refugees to the United States. Citizenship refers to a specific country or countries of which the actor is a citizen, ancestry refers to a country by which the actors' ethnicity can be traced, for a maximum of two generations, and refugee status is a dichotomous variable to discern whether they have ever been a refugee.

Educational: As with economic factors, there has been conflicting information regarding the education levels of terrorists. Research has found terrorists to be relatively well-educated, with the vast majority completing secondary education, and a sizable number completing a university degree (Sageman 2004; Bakker 2006; Gill et al. 2015). In some instances, like that of Palestinian suicide bombers, they have a higher rate of education than the general population (Berrebi 2007). There are two variables, one dichotomous to establish whether the actor was enrolled as a student in tertiary education (such as university or community college) at the time of their event, and one categorical to establish the highest level of education they achieved.

Criminal Record: It has also been found that terrorist actors have a higher rate of criminal interactions than the general public (Bakker 2006; Vidino et al. 2017; Horgan et al. 2016). This research will firstly code dichotomously whether the actor had been convicted of a crime (felony or misdemeanour) and then categorically regarding the type of crime.

Convert: Research has found that converts to Islam make up a disproportionately high proportion of jihadist terrorists (Azani and Koblentz-Stenzler 2019; Kleinmann 2012; Fodeman, Snook, and Horgan 2020). To either confirm or challenge these findings, this dichotomous variable will establish whether there is evidence to show that the actor converted to Islam.

Mental Illness/Learning Disability: The idea that terrorists suffer from mental illnesses has a long history in Terrorism Studies, which has largely suffered from the debate not being driven by data (Corner and Gill 2018). This research takes the lead of Corner, Gill and Mason (2016) by disaggregating different types of mental health and learning disability rather than treating the phenomena as a monolith. There are two variables; the first categorical to distinguish if mental health/learning disabilities have been diagnosed;

are credibly speculated to be present; or are not present. Secondly, a categorical variable which lists the 17 types of mental health problems or learning disabilities that are used by Corner, Gill and Mason (2016).

Network Behaviours

Co-Offenders: It is often suggested that the nature of terrorism has changed, with traditional terror groups becoming less common (Post 2015). This variable collects data for how many actors were involved in the direct execution of the plot; this does not include those that only offered facilitative support such as loaning money. It takes the lead of Corner, Gill and Mason (2016) who demarcate into four categorical variables based on group sizes: Lone Actor – one that acts and plans entirely alone; Solo Actor – one that acts alone but does so at the direction of a larger group; Lone Dyad – two that act alone; and Group Actor – members of a wider network of more than two.

Online Contact with Co-Ideologues: One of the key variables of disaggregating "online radicalisation" in the database studies of Gill and others (Gill and Corner 2015; Gill et al. 2015, Gill 2016; Gill et al. 2017). This dichotomous variable encompasses every kind of online interaction with co-ideologues, which will be further disaggregated below.

Reinforce Beliefs/Disseminated Propaganda/Provided Support to Others/Sought Legitimisation/Attack Signalling/Recruiting Others – Online: Variables for these six dichotomous online behaviours are collected to mirror that of Gill et al (2015), outlined above.

Online Link to IS: This dichotomous variable codes for whether the actor made online contact with members of IS within their territory. Research has suggested that a team of "Virtual Entrepreneurs" operated out of Raqqa, giving operational support to actors in the West (Hughes and Meleagrou-Hitchens 2017). This variable can help demonstrate the extent to which this is the case and the impact that it had.

Shared Ideology Online: Research has suggested that IS was able to effectively leverage social media platforms to spread their message to wide audiences (Berger and Morgan 2015; Carter et al. 2014; Ingram 2014; Winter 2015b). This dichotomous variable seeks to identify whether the actor shared their ideological beliefs in an open or semi-open forum; for example, Twitter or Facebook "posts" but not private messages on either platform.

Offline Contact with Co-Ideologues: Gill et al. (2017) find that engagement in virtual interactions with co-ideologues was significantly correlated with similar offline interactions. This has important implications for "online radicalisation", as it suggests that terrorists tend to act in both domains. As such, this dichotomous variable will be used to either confirm or challenge that finding.

Social Media: IS' use of mainstream social media platforms, such as Facebook (Carter et al. 2014; Waters and Postings 2018) and Twitter (Berger and Morgan 2015; Pearson

2017) is well-documented, but research suggests that IS may utilise dozens (Conway et al. 2017) or even hundreds (Tech Against Terrorism 2019) of different online platforms. There are two variables: one dichotomous as to whether there is evidence of social media use for purposes related to the event or to communicate with a network, and one string variable to document which social media platform was used.

End-to-End Encryption: As well as open social media platforms, research has found that IS have utilised end-to-end encrypted platforms such as Telegram (Bloom et al. 2017) and there is evidence to suggest that they may be using the Dark Web (Malik 2018) and cryptocurrencies (Azani and Liv 2018; Malik 2018). This dichotomous variable codes for whether there is evidence to suggest that end-to-end encrypted technology has been used. This can also be tested for significance against the date of arrest/event to ascertain whether use of end-to-end encryption has become more prevalent in response to mainstream platforms' tougher regulatory stance (Conway and Courtney 2017; Macdonald, Correia, and Watkin 2019).

Tried to Recruit Others Offline: As a sub-variable of "engaging with co-ideologues offline", it is worthwhile to attempt to discern whether attempted recruitment has a significant correlation between the online and offline milieu.

Event Behaviours

Date of Event/Arrest: This variable collects the date on which the actor successfully executed their plot, died or was charged. This can be used to assess whether behaviours have changed over time. For example, the observation that IS actors moved to Telegram after 2016 saw mainstream social media platforms take a tougher regulatory stance (Conway and Courtney 2017; Macdonald, Correia, and Watkin 2019).

Role in Event: As well as disaggregating the role of the Internet, it is also important to understand that the notion of a terrorist is not homogenous. Gill et al. (2015) argue that it is instructive to disaggregate terrorist offenders into discrete groups to ascertain whether behaviours are different for separate roles. This categorical (and multiple entry) variable splits "terrorist" into five roles: Attacker, Traveller, Financier, Facilitator, and Bomb-maker.

Attack Methods: For those that attacked (successfully or unsuccessfully), it is also important to ascertain the methods that were used. This can be used to test whether Internet usage is more likely with some behaviours than others, as Gill et al. (2015) find; those that used/plotted with an improvised explosive device were significantly more likely to have learned online. This categorical (and multiple entry) variable has four sets: Armed assault, Unarmed assault, Improvised Explosive Device, and Vehicle-based.

Attack Targets: As with the method of attack there is value in ascertaining the target. For example, Gill et al (2015) find that those that target the government were significantly

more likely to have learned online than not. This categorical (and multiple entry) variable is demarcated into four answers: Government, Civilian, Military, and Police.

Deadly Attack: One of the ways to measure the risk of terrorism is to determine whether it causes death. Online behaviours can be tested against this dichotomous variable to ascertain whether online learning or communication makes killing others more or less likely. Gill and Corner (2015) find that offenders that make use of online learning were significantly less likely to kill.

Learned/Planned Online: As with online communication with co-ideologues, this is a key variable in Gill and Corner (2015) and Gill et al. (2015), and is a catch-all variable for any kind of online learning or planning, which is further disaggregated below.

Access Ideological Content/Online Motivation/Choose Target Online/Prepare Event/Overcome Hurdles: Variables for these five dichotomous online behaviours are collected to mirror that of Gill et al (2015), as outlined above.

Learned/Planned Offline: As with offline interactions with co-ideologues, Gill et al. (2015) find that the online learning or planning of terrorist attacks is significantly correlated with its offline equivalent. This has important implications for "online radicalisation", as it suggests that terrorists tend to act in both domains. As such, this dichotomous variable will be used to either confirm or challenge that finding.

Divulged Online: It has been found that terrorist actors, particularly lone actors, often divulge their plans to those close to them (Schuurman et al. 2018; Bouhana et al. 2018). This categorical variable assesses whether the actor divulged their plan online; either partially/vaguely, or with specific details.

Divulged Offline: This mirrors the above variable, except with admissions of the actor's plan in the offline domain.

Successful: A further measure of risk is whether the attack/event is successful (i.e. an attack coming to fruition or an actor travelling to the caliphate). As with the variable for "Deadly Attack", this can be tested against online behaviours to ascertain whether it helps facilitate events or acts as an impediment, as suggested by Jensen et al. (2018). An attack is considered successful if it occurs, regardless of injuries and fatalities. For example, the attack in Garland, TX by Elton Simpson and Nadir Soofi is considered successful because they began the attack before being shot dead.[19]

Known to Authority: This dichotomous variable determines whether the actor was known to the security services for reasons of terrorism/extremism. Often, it is claimed that terrorists are known to the security services prior to their event (For example, see:

[19] Catherine Shoichet and Michael Pearson, Garland, Texas, Shooting Suspect Linked Himself to ISIS in Tweets, *CNN*, May 5, 2015. Available at: https://edition.cnn.com/2015/05/04/us/garland-mohammed-drawing-contest-shooting/index.html.

Sullivan and Wan, 2016). This will help determine a picture of how many of the IS actors in the US were on the law enforcement radar.

Undercover: Greenberg and Weiner (2017) find that between 2014 and 2017, the number of IS-related prosecutions that include an undercover agent of some kind rose from 33% to 83%. Horgan et al. (2016) find, in their sample of US-based terrorist offenders that around 50% had come into contact with an undercover officer. This dichotomous variable discerns whether there was any undercover actor (either an agent or a paid informant) that was pretending to be part of the conspiracy.

Post Event Behaviours

Arrested: This dichotomous variable codes for whether the actor was arrested as part of their activity. This will help create a picture of whether certain behaviours make arrest more likely.

CJS Details: For the actors that are charged in the US Criminal Justice System, this categorical variable details the status of the actor: whether they have merely been arrested, charged; convicted; acquitted; pleaded guilty; or had charges dropped.

Crime Charged: For those that have been charged in the US Criminal Justice System, this string variable collects the name of the crime. Greenberg and Weiner (2017) find that a single crime – Material Support for a Designated Foreign Terrorist Organisation – is relied upon heavily for IS cases, while Berkell (2017) finds that the provision has increased dramatically in recent years.

Sentence: For the actors that have been given a custodial sentence, this variable details how long it was in months.

4.6 Analysis

4.6.1 Quantitative

After the second round of coding, the database consists of several quantitative variables, which are mostly categorical in nature. In most cases the categorical variables are binary, such as when behaviour is either present or not – i.e. whether there is evidence to suggest the actor used the Internet to learn about their intended activity or not. As with the creation of the codebook, I follow the lead of Gill and others by conducting a descriptive analysis as well as several bivariate tests such as chi-square analyses and Fisher's Exact Test (Gill and Corner 2015; Gill et al. 2015; Gill 2016; Gill et al. 2017). The descriptive analysis yields the frequency with which each variable occurs within the sample; for example, the percentage of actors that used the Internet to engage with co-ideologues. Because the quantitative aspect of this research is, in large part, replicating the codebook and methods of Gill and others, many of these variables can be directly compared to assess the differences between the two terrorist populations' Internet usage.

Chi-square analyses test the relationship between two categorical variables by comparing the frequencies in the categories against the frequencies that one might expect given a random distribution; if the *p* value is less than 0.05 then the null hypothesis (that the variables' relationship is randomly distributed) can be rejected (Field 2018). For example, in Gill et al (2017), they find a significant correlation between those that engaged in a virtual network and those that engage in an offline network – both instances occurred in 58.2% of cases, which has a *p* value of 0.000. Therefore, they reject the null hypothesis that there is no relationship between the two behaviours.

One problem with chi-square analyses is that they require the expected frequencies for each cell to be at least five, or else the sampling distribution is too low for the chi-square distribution to be accurate (Field 2018). Fisher's exact test is a solution to this problem, computing for smaller sample sizes which would be problematic using a chi-squared analysis. For example, if two dichotomous behaviours – online interaction with co-ideologues and warning about their intended activity – are being analysed, but there are so few instances of the latter behaviour that the expected count is below five, Fisher's exact test would be appropriate. Although it can be used for any sample size or larger contingency tables, it was designed specifically for smaller samples for which the chi-square approximation would be inaccurate (Field 2018).

In some cases, online behaviours are tested against other types of variables. For example, it was deemed instructive to determine whether younger actors used the Internet more than their older counterparts. Analysis of variance (ANOVA) tests are used to test a continuous response variable against discrete categorical groups, comparing variance among groups relative to variance within groups (Larson 2008). In the example given above, it would assess the mean ages for individuals that used the Internet and for those that did not and compare the variance between them. The null hypothesis is that there are no differences between the two groups, therefore, a statistically significant response (*p = <.05*) suggests that one group is, in fact, more likely to use the Internet, and one would reject the null hypothesis.

A series of binary logistic regressions are also conducted. This refers to a model for predicting dichotomous outcomes from categorical or continuous variables. That is to say, it analyses the simultaneous effect of multiple factors on a single outcome (Ranganatham et al. 2017). For example, the chi-square analyses show that there are significant relationships between the use of the Internet and the success of actors' plots. Therefore, a binary logistic regression is used to establish whether a specific type of online behaviour predicts success (or lack thereof). This is done by first calculating a baseline which represents the odds of the binary outcome (in this case success) happening without any predictors – this is called the constant. Then the independent variables are added (different online behaviours) and a regression coefficient and a *p* value is calculated. If the *p* value is less than 0.05 for any independent variable then it contributes significantly to the occurrence of the outcome – in this case, the success of the terrorists' event (Ranganatham et al. 2017).

The results of the quantitative analyses are important for two reasons. Firstly, the database studies of Gill and others conclude that the significant relationships between many online and offline behaviours casts doubt on the online/offline dichotomy in pathways towards terrorism (Gill et al. 2017; Gill et al. 2015; Gill and Corner 2015; Gill 2016). Given the dearth of data-driven research, results that either confirm or conflict with this conclusion will be important. Secondly, the results will be important in their own right, offering a snapshot of contemporary Islamist terrorism within the US; with the iterative aspect of coding offering new insights.

4.6.2 Grounded Theory

The quantitative measures outlined above offer an important view of the sample as a whole, but in many instances, the data are too complex to analyse with a binary coding system. As a result, an inductive approach is also taken to the research. While conducting the first and second round of quantitative coding described above, the data were also simultaneously coded using a methodology inspired by Grounded Theory (GTM). In contrast to the deductive[20] nature of coding and analysing data against a pre-existing codebook against a null hypothesis (such as the independence of categorical variables in a chi-square analysis), GTM is an inductive method of inquiry, dating back to Glaser and Strauss' *The Discovery of Grounded Theory: Strategies for Qualitative Research* (1967). The authors believed that much could be learned from generating theories from the data if they the researcher is not incumbered by existing theory.

Importantly, rather than fixed research questions, such as the four that were identified for quantitative analysis, GTM starts with a general area of interest (Lehane 2017), which in this case is the phenomenon of online radicalisation. This process occurs via three rounds of coding: Firstly, *open coding* in which the researcher codes the data according to any emerging theme that they identify, then *selective coding* in which the original codes are grouped into larger categories for the basis of comparison, and finally, *theoretical coding*, where these categories are considered in relation to each other for the ultimate goal of GTM – theory building. The data were coded using NVivo, a software package designed for the storing and analysis of qualitative data. Although NVivo has an "Automated Insights" function for coding, it is not utilised in here because it is designed for fast results that could be inaccurate. As this research requires line-by-line data analysis, manual coding is the most appropriate method (NVivo nd a). However, other automated elements of the software are used, such as running word frequency queries once potential themes have been identified (NVivo nd b).

The presentation of findings in GTM typically differs quite substantially to deductive research, with the authors' thought process and decision-making elucidated throughout the work. Therefore, the methodological considerations for this analysis can be found at the start – and throughout – Chapter 6.

[20] Note that the iterative nature of the second quantitative code means that it is not purely deductive.

4.7 Ethical Considerations

Before proceeding to the results, it is important to discuss the prescient ethical considerations when undertaking terrorism research. One might assume that because all the data are collected via open sources, there are minimal issues because there is no direct contact with research subjects and therefore there are fewer, or no, safeguarding issues. However, there are several considerations that must be addressed.

4.7.1 Identifying Research Subjects as Terrorists

Although there is no direct contact between the researcher and research subject, the former can cause a substantial amount of personal damage to the latter if they are publicly named as a terrorist, given the value-laden nature of this word. Many individuals in this sample are either the subject of ongoing legal proceedings or were never formally charged, and many have died so there is no chance of them being convicted. This raises a difficult problem. If the present study were to only include individuals that have been convicted it may create a skewed sample, particularly given that an important variable is whether the actor was successful.

For the quantitative analysis, where results are reported numerically, this is not problematic as long as identifying information is not presented. However, for the GTM analysis, this could be an issue. It is typical for qualitative research to protect research participants' privacy by anonymising or pseudonymising the data, but this is not possible here because the findings must be referenced for academic rigour. The most appropriate way of proceeding is to make note of cases that are ongoing or unresolved during the coding process and to reference the state of the case when discussing the findings. For example, Abdi Nur, who is thought to be deceased, is *alleged* to have left Minneapolis for Syria in May 2014. Similarly, the only actor that has been acquitted – Noor Salman – was removed from the database. While no situation is perfect at remedying the ethical tension between conducting robust research and protecting participants, this tactic mitigates potential harm to an acceptable level.

4.7.2 Data Storage

It is also important to consider the ethics of storing and processing personal data without the consent of the research subjects, which can be unlawful in certain contexts. Given that this research was conducted within the United Kingdom and the Netherlands between 2016 and 2019, the data storage was obliged to conform to the European Union General Data Protection Regulation (GDPR). Importantly, the GDPR does offer an exemption, permitting the processing of personal data if it 'is necessary for the performance of a task carried out in the public interest' (General Data Protection Regulation, 2018, Article 6 (1) (e)). Terrorism, particularly in the online domain, has repeatedly been affirmed as a top priority by most governments, including those of the United Kingdom and the Netherlands (HM Government 2017; Rutte 2017), as well as at the European level (Council of Europe 2014). During the research, data were stored in an encrypted USB and

all software was protected by a password and undertaken in a room with electronic key card access.

4.7.3 Researcher Self-Care

A final important ethical consideration is that of self-care, particularly given that the topic of terrorist activities online contains a great deal of gruesome, distressing, and violent content. Even research which utilises open-source data, like this project, can take a toll. At times, court documents contain disturbing images of injuries sustained due to terrorist attacks or may include still images from propaganda videos. As such**,** it is important to create an environment in which such matters can be discussed. Fortunately, both universities in which this research was undertaken have formal services – such as student wellbeing centres – and informal environments, such as research communities in which potentially distressing content can be discussed.

An interrelated point is that of staying within the confines of the law. Most of the research was conducted within the United Kingdom, in which an individual can receive a sentence of up to fifteen years for accessing terrorist propaganda (Counter-Terrorism and Border Security Act 2019), but much of the research was focused on US court documents, in which the legality of terrorist propaganda is less clear (Raban 2018). Many of the court documents include propaganda which would be considered illegal in the United Kingdom. Academic research is considered a reasonable excuse for possessing such propaganda (Counter-Terrorism and Border Security Act 2019), but as an extra level of security, the local police in the United Kingdom were contacted and informed about the ongoing research.

This project was granted ethical approval by the Swansea University School of Law Ethics Board in the spring of 2017.

4.8 Conclusion

The research that follows is an analysis of the online behaviours of IS actors in the US. This chapter has laid out the research design, methods of data collection, inclusion and exclusion criteria, coding system, and the methodological considerations for the quantitative and GTM analyses. It concludes by offering several ethical issues that must be considered when undertaking research within this field. The research will provide two important empirical contributions to the literature, firstly, by developing a codebook from the academic literature and testing it against a sample that has not yet been the subject of rigorous, data-driven analysis. Secondly, it makes a new contribution by establishing theories which are grounded in the data which can be tested in future.

Chapter 5: Quantifying the Online Behaviours of Islamic State Terrorists

5.1 Introduction

Having collected data on every named IS actor within the US and applying the inclusion and exclusion criteria laid out in Chapter 4, the database is made up of 201 terrorists. After offering a descriptive snapshot of the sample's demographics and a comparison to other database studies, this chapter will answer the four research questions identified in Chapter 3:

> *RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?*
>
> *RQ2: Has the Internet replaced the offline domain as the primary venue for terrorists' antecedent behaviours?*
>
> *RQ3: Do terrorists that use the Internet exhibit different experiences to those that do not?*
>
> *RQ4: Does using the Internet help or hinder plots?*

These questions are taken in turn before turning to a discussion of their findings and integration into the academic literature. This chapter demonstrates that terrorists use the Internet heavily for a range of pre-event behaviours. However, this should not necessarily be taken as evidence for an "online radicalisation" thesis; bivariate tests show that the online realm is not replacing the offline and that, for the most part, those that use the Internet do not exhibit different behaviours to those that do not. Finally, despite the claims that the Internet could be a security risk by radicalising would-be terrorists, the findings of this chapter suggest that those that use the Internet are less likely to be successful than those that do not.

5.2 Demographic Snapshot

Before turning to online behaviours, it is instructive to offer a descriptive account of the sample. This is important for two reasons: Firstly, it gives an insight as to whether the IS actors in America are similar to previous database studies. This could be useful in explaining differences in online behaviours. For example, if the average age was meaningfully younger than in other studies, that may explain a higher Internet usage. Secondly, demographic factors can be analysed using bivariate and multivariate tests against online behaviours, answering questions such as whether female actors use the Internet more than men. After discussing demographics, several descriptive event behaviours that do not relate to the Internet are presented, such as the number of actors involved in a plot; the date of the event; and interactions with the criminal justice system. These too are used as part of the analysis, such as establishing whether online behaviours have increased over time.

The 201 IS actors identified in the sample are predominantly male (90%), which is in keeping, if not slightly lower than other database studies, which have been above 95% (Horgan et al. 2016; Bakker 2006; Sageman 2004; Gill et al. 2015). From the 197 actors whose age could be identified, the average is relatively young (Mean: 27.5; Median: 26; Mode 20), it spans an range of 15-55 (Figure 6).[21] This age range is remarkably similar to Gill et al. (2017), who find a mean of 28; a median of 27; and a mode of 22; with an age range of 16-58 – the similarities between these demographic factors make the two databases ripe for comparison. Similarly, Sageman finds a mean age of 25.7 years, while Bakker's sample is 27.3 years. This places the age of the sample squarely in the centre of the previous literature; a male-predominated cohort, primarily in their twenties, but with a wide age distribution.

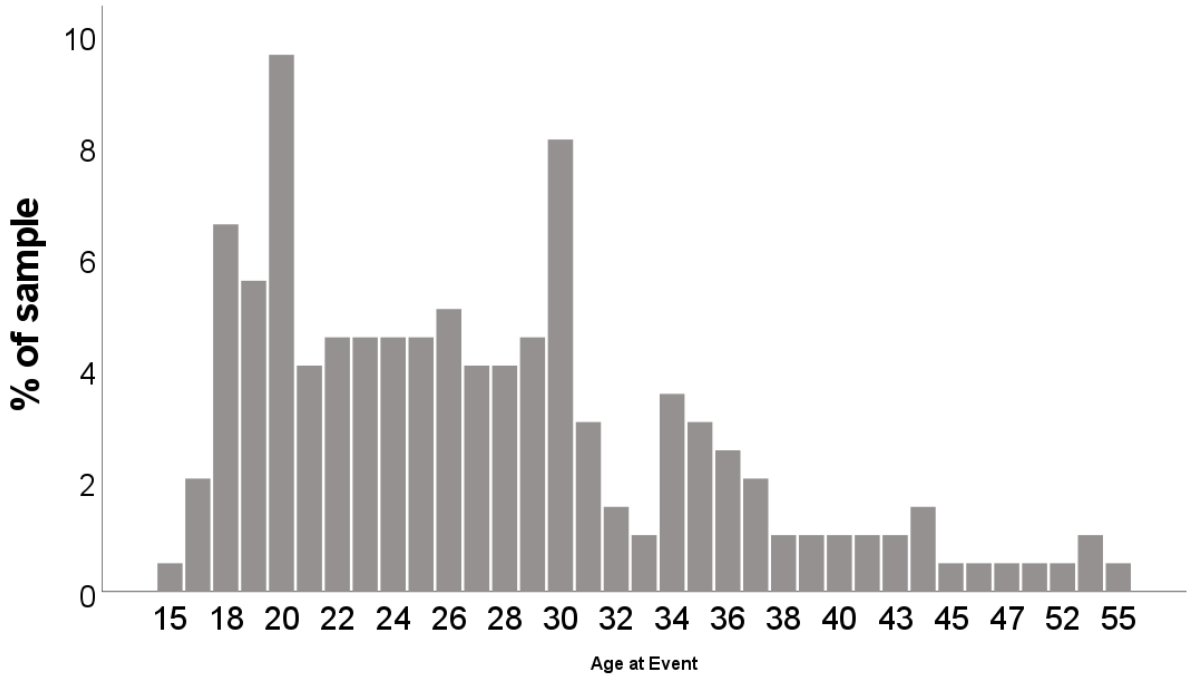


Figure 6 - Age at Event

Employment variables suggest that while the group err towards the lower end of the economic spectrum, it is still relatively heterogeneous. Two data points for employment were collected: Firstly, a dichotomous variable for whether the actor was employed, of which evidence was found for 49%. Next, of the results that showed data (n=122), this was broken down categorically over five variables – Not Employed (29%),[22] Service/Low Skilled (48%), Professional (11%), Student (9%), Armed Forces/Police/Federal (3%) (Figure 7). At first glance, this level of unemployment is substantially larger than the US

[21] This sample includes only 3 actors under the age of 18 because they were charged as adults. Given it is standard practice for criminal justice information not to name minors (if they are going through a youth justice process), it is possible that this age range and average undercounts the true figure. However, it seems prudent to demarcate between those tried as adults and those that were not. There were no travellers under the age of 18 aside from the unnamed children of other actors.

[22] Unlike the above variable, explicit mention had to be made that the actor did not have a job.

unemployment rate which has gradually trended down from 8% to 3.5% in the years 2012 to 2018 (BBC 2019). However, it is worth noting that this is not comparing like-for-like. Unemployment rates track those who are not employed but are willing and able to work, while this study coded for affirmation of a lack of employment. Pew find that 40% of US Muslims say they are not currently employed and 18% are looking for work (Pew Research Center 2017a). Although an age distribution is not possible, the data suggest that this sample is roughly aligned with what one might expect given a random distribution. This too is in keeping with other research: Gill et al. (2015) find that one-third of their sample is unemployed, and both Horgan et al. (2016) and Gill et al. (2015) report 12% and 14% students respectively.

Similarly, the highest level of education (n= 120) attained paints a similar picture, with a majority achieving a high school diploma (64%), and the next highest group having not finished high school (18%) - Figure 8. Only 12% had a bachelor's degree, while 5% achieved a postgraduate degree. This sample seems less educated when compared to the wider US Muslim population, of which 31% have a college degree (Pew Research Center 2017a). However, this does not account for age – several actors in this sample are too young to have successfully completed university. These numbers are strike a difference with Horgan et al. (2016), 14% of whom high school was their highest qualification, although they report a high number completing an undergraduate degree (22%) and postgraduate (10%).

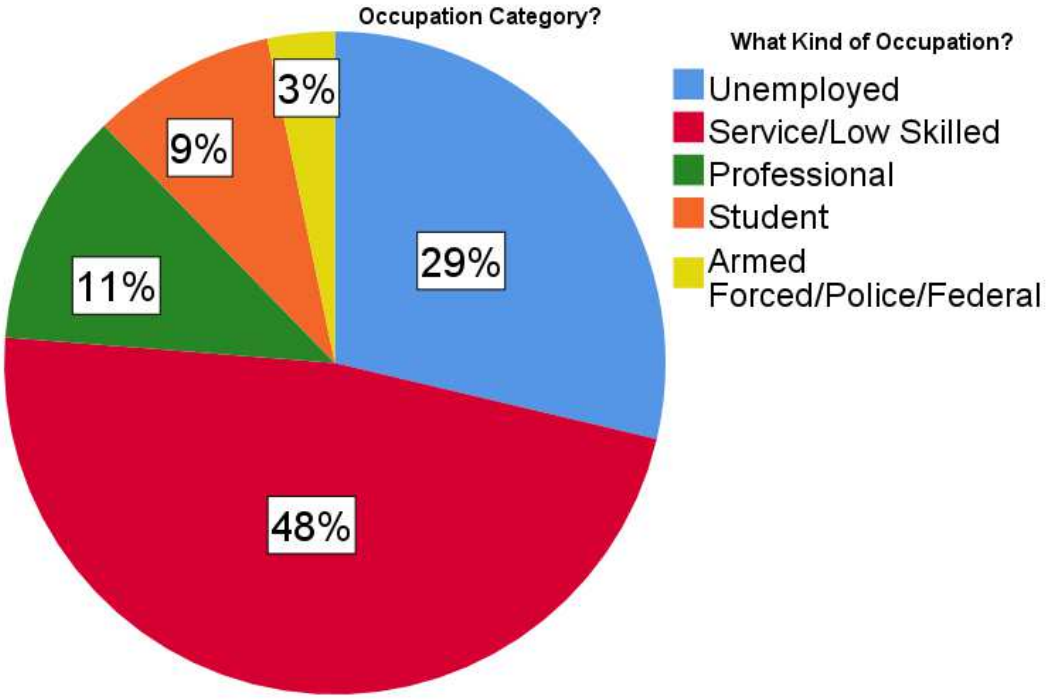


Figure 7 - Occupation

It has been posited that there is a link between economic factors and terrorism, although the evidence is inconclusive (For example, see: Piazza 2006; Piazza 2011; Cruz et al. 2018). However, income and wealth are difficult variables to collect data for when

conducting open-source research as it is often not reported and requires too much of a subjective judgement on the part of the coder (Bryson 2017). Therefore, employment and education factors offer the best insight. The data suggest that while there does appear to be a greater weighting towards those at the low-skilled end of the economic spectrum, no group is excluded entirely.

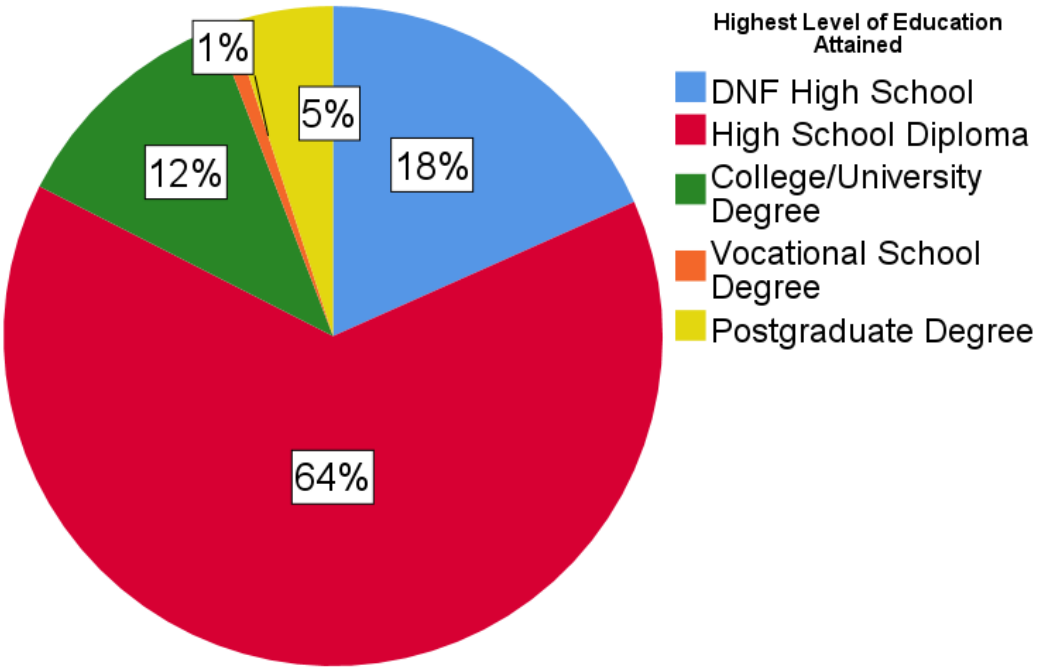


Figure 8 - Highest Level of Education

With regards to family characteristics, the majority – 60% - were single (or data to suggest they were not single could not be found); 33% were married or had a long-term partner, while 8% were divorced or separated. This is somewhat lower than Horgan et al. (2016) who found that 48% were married or had a partner and 9% were divorced. Similarly, around one third of the sample had children, which too, echoes Horgan et al.'s research. One variable that is not included in previous literature which may be instructive is the actor's family characteristics growing up (n=87): 61% were reported to have grown up in two-parent families; while 24% by single-parents; and 14% spent significant time in their childhood being raised by someone who was not a parent.

There are a wide range of countries of birth (n=197) represented in the sample, with the USA being by far the most common. Almost two-thirds were born on US soil, suggesting that the primary threat is from homegrown, rather than transnational, terrorists. No other country is represented in more than 4% of cases, with notable countries being: Bosnia (4%), Uzbekistan (4%), Somalia (3%), Bangladesh (3%); Kenya (3%),[23] Iraq (2%). To further highlight the homegrown nature of the threat, 83% of the sample were either a full US national or a US dual national from 197 cases with identified nationalities. Again,

[23] All five of those born in Kenya were born in a Somali refugee camp.

no other country is represented in more than 4% of cases. Even when considering ancestry (of a maximum of two generations), America is still by far the highest represented country at 45%, with Somalia at 11%, and Pakistan, Bosnia, Uzbekistan, and Yemen at 4%.[24]

The vast majority (92%) were residing in the US at the time of the event, which is intuitive given the rigorous inclusion criteria described in Chapter 4. Examples of those that were not include those that committed events that were heavily reliant on the Internet, such as Russel Salic, who transferred money for a US-based plot from the Philippines or those that plotted over international borders, such as Abdulrahman El Bahnasawy – the recipient of Salic's money, who resided in Canada and planned an attack over the border in New York City.[25]

The city and state of residence of the actor offer instructive findings. Much of the literature that plays down the role of the Internet suggests that offline networks or "radicalisation hotspots" may play a bigger role (Reynolds and Hafez 2017; Vidino et al. 2017; Soufan Group 2015). Although 94 cities from 196 cases are identified, only two make up sizable shares: New York City (11%) and Minneapolis (9%), with the rest all under 3%. When identifying the state of residence (n=185), over 30 states (plus Washington D.C.) are found, and a number make up sizable proportions: New York State (13.5%); Minnesota (10%); Virginia (10%); California (9%); Florida (6%); Ohio (6%); and Texas (6%).

The distribution of cities or states does not in itself entail a highly networked movement, particularly in states with large populations (such as New York) and diffuse cities (such as California). That being said, the vast majority of the actors in Minneapolis, MN, are noted to be a highly networked group of individuals of Somali descent that played important roles in each others' successful and attempted travel to Syria and Iraq.[26] Similarly, although there are a number of different plots in New York City, a sizable proportion is represented by the six men of Uzbek descent that financed and facilitated the attempted travel of Akhror Saidakhmetov.[27] Conversely, looking only at the frequencies by state also fails to observe clear offline networks, such as the one that successfully facilitated and financed Abdullah Ramo Pazara's travel,[28] and the group of

[24] It should be noted that if there was no evidence to suggest that actor had ever left the country that they were coded as being born in America and being a US citizen, making these variables quasi-default. However, these cases are relatively rare as criminal justice documents often explicitly make mention of citizenship.
[25] USA v. Russel Salic, Criminal Complaint, [No Case Number], United States District Court for the Southern District of New York, 2016.
[26] USA v. Mohamed Abdihamid Farah et al. Criminal Complaint.
[27] USA v. Abdurasul Juraboev et al., Superseding Indictment, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York, 2015.
[28] USA v. Ramiz Hodzic et al. Government's Response in Opposition to Defendant's Motion to Dismiss, Case: 4:15-cr-00049-CDP-DDN, United States District Court for the Eastern District of Missouri, Eastern Division, 2015.

young men that lived across the New York State and New Jersey border that both plotted an attack[29] and planned to travel.[30]

Several other variables provide an instructive insight into the demographics of the database. Refugees make up 8% of the sample, which while small in proportion to the whole database, is almost certainly higher than the proportion of refugees against the total US population, which is estimated to be at least 0.3% (Alpert 2017), although the true number is difficult to establish.[31] One explanation for this may be found in Piazza's research on predictive causes of transnational terrorism: He suggests that failed states (which refugees are from by definition) produce significantly more terrorists than those that do not (Piazza 2008). This research seems to support this notion, given that Somalia is the second most frequently occurring country in terms of birth (when including the Somalis born in Kenyan refugee camps) and ancestry; Somalia is currently in the highest bracket of "Very High Alert" in the 2019 Fragile State Index. In fact, all of the five Muslim-majority countries in "High Alert" and "Very High Alert" in the index are represented in this sample: Yemen, Somalia, Syria, Afghanistan, and Sudan (The Fund for Peace 2019). This is also in keeping with research that suggests that exposure to conflict increases stress, which in turn hardens attitudes and evokes a feeling of threat (Canetti et al. 2013).

Twenty-nine percent of actors in the sample converted to Islam, higher than the one-quarter presented in Horgan et al. (2016), but lower than the 37.3% of al-Qaeda inspired actors in Gill, Horgan and Deckert's (2014) sample. The number in this sample is slightly higher than one might expect given the estimated 23% of American Muslims that are converts (Mohamed and Scuipac 2018). It should be noted that because this methodology requires explicit mention of an actor converting, it almost certainly undercounts the true number. There are a number of actors for whom, demographically, it is very likely they converted but could not be coded as such. The place and roles of converts to Islam within violent extremism occupies an interesting, yet mostly unanswered, space. Many scholars have noted that the total number within violent Islamist movements has increased in recent years (Sedgwick 2010; Hafez and Mullins 2015; Klausen 2016b), but it is not clear why. Kleinmann's research on Sunni Islamist terrorists within the US finds that the trajectories that actors go through, particularly at the individual level, may be fundamentally different to non-converts. Halverson and Way suggest that the mystique of Islam offers disaffected and potentially violent individuals a new identity (Halverson and Way 2012), while Hafez and Mullins note that many come from backgrounds of crime and are knowledge-hungry, restless and susceptible to promises of an afterlife (Hafez and

[29] USA v. Fareed Mumuni, Criminal Complaint, Case 1:15-mj-00554-VMS, United States District Court for the Eastern District of New York, 2015.
[30] USA v. Samuel Topaz, Criminal Complaint, Case 2:15-cr-00450, United States District Court for the District of New Jersey, 2015.
[31] The US Government tracks the number of those that have resettled to America, but does not appear to track after they have become lawful permanent residents or naturalised citizens. The above estimate is based on how many refugees settled in America from October 2001 – April 2017. The actual number is almost certainly higher, but it is reasonable to assume that it is not close to 8%.

Mullins 2015). If there is an overrepresentation of converts to Islam within the sample, there is no obvious determinant of the relationship. That is to say, it is not clear whether it is something about the people that convert or something about Islam as a host that leads them towards political violence.

Around one quarter of the sample have a previous criminal record. However, it should be noted that only 5 of the 48 cases (10%) were for charges pertaining to terrorism. Rather, the majority of the charges are for what could be described as petty crimes, including nine instances of theft (19%), eight drug crimes (18%) and eighteen (40%) that were categorised as "other misdemeanour", which includes crimes such as simple assault and driving offences (Figure 9). This suggests that the sample is not made up of battle-hardened terrorist veterans, but rather the majority have had minimal involvement with the criminal justice system, and where they have, their crimes tend to be at the less-serious end of the spectrum. This seems to mostly follow the thesis of Basra, Neumann and Brunner (2016), who posit a crime-terror nexus, suggesting that a large number of terrorists in Europe have low-level criminal backgrounds, but this life in crime may have given them a number of important skills, such as understanding how to deal with law enforcement.

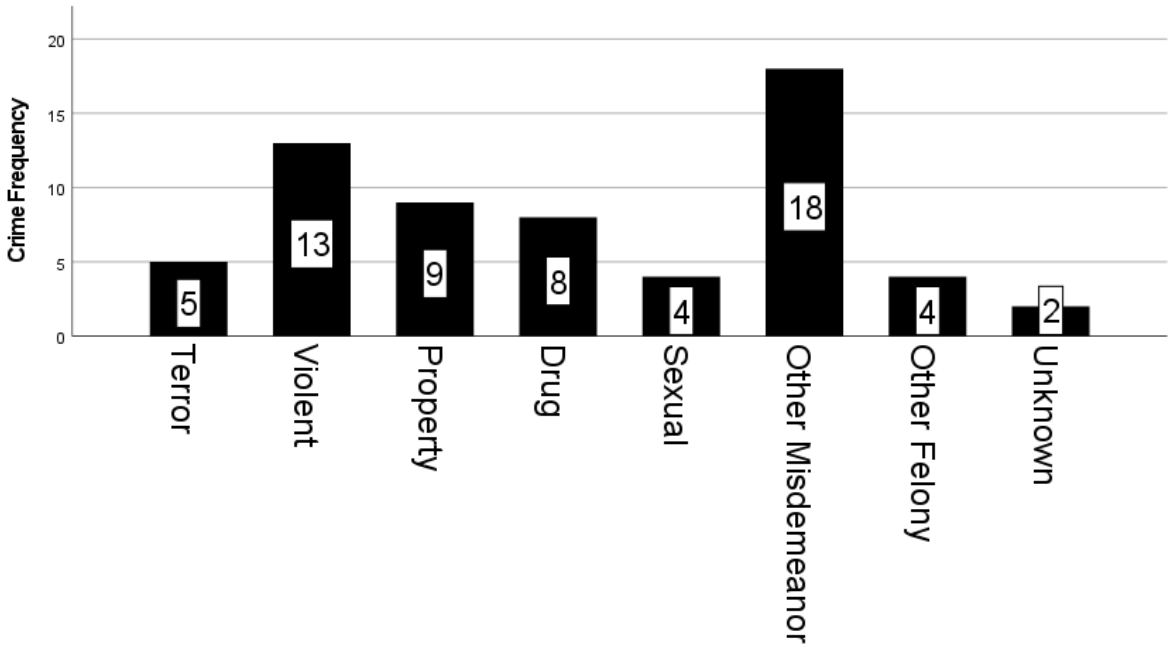


Figure 9 - Criminal Record

The majority of the sample – around three-quarters – do not have an identifiable mental illness. Two data points were used to ascertain whether an actor does suffer from mental health issues. Firstly, if there is evidence of a professional diagnosis, and secondly, if there is credible speculation, such as testimony from family or defence counsel, which is a less reliable measure. Twenty-two (11%) have been professionally diagnosed, while it was credibly speculated in twenty-six cases (13%). The combined total of both (24%) is

almost exactly equal to the proportion of the American population offered by the US-based National Alliance on Mental Illness, who suggest that 46.6 million – roughly one in five – experience a mental illness in a given year (National Alliance on Mental Illness nd). Following the advice of Corner, Gill, and Mason (2016), these results are further disaggregated by different type of mental health disorder into seventeen different categories. Depression and schizophrenia are first and third most frequently occurring in the sample, which is similar to the findings of Corner, Gill, and Mason, but their sample has few instances of drug dependence, which is the second most frequently occurring in this sample. Full results can be seen in Figure 10. It is important to note that even if there is a prevalence of mental health issues, this does not imply a causative relationship between the issue and engaging in terrorism.

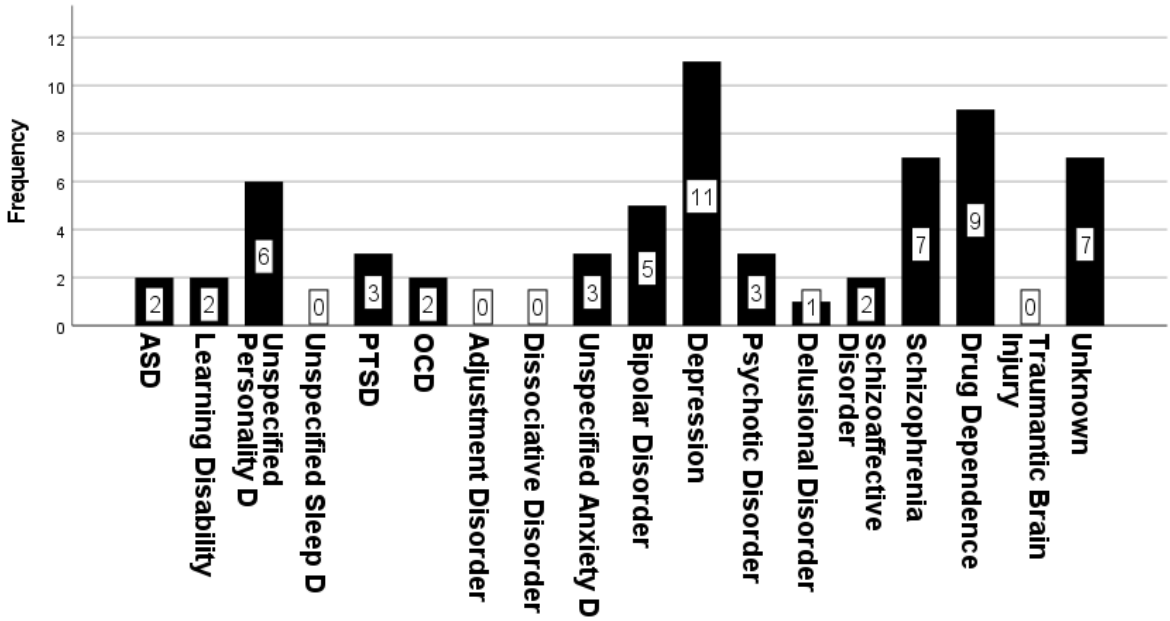


Figure 10 - Type of Mental Health Problem

The dates of the event – when the actor is charged; successfully conducts an attack; or successfully leaves the US – are heavily skewed towards 2015 (as can be seen in Figure 11) with a mean of October 31st 2015 and median of July 10th 2015. In total 77 of the 201 events (38%) occurred in 2015, with each other year registered at under 20%. IS was undoubtedly at its peak in 2015, controlling extremely large territories in Iraq and Syria, as well as conducting large scale terror attacks in the US,[32] France,[33] Tunisia,[34] and many

[32] BBC News, San Bernardino Shooting: The Story of the Attack, December 5 2015, Available at: https://www.bbc.co.uk/news/av/world-us-canada-34991990/san-bernardino-shooting-the-story-of-the-attack.
[33] BBC News, Paris Attacks: What Happened on the Night, December 9, 2015, Available at: https://www.bbc.co.uk/news/world-europe-34818994.
[34] BBC News, Tunisia Attack on Sousse Beach 'Kills 39', June 27, 2015, Available at: https://www.bbc.co.uk/news/world-africa-33287978.

others. It seems plausible that this peak would have made the group seem popular to potential suitors, as well as increasing the number of law enforcement resources devoted to apprehending them.

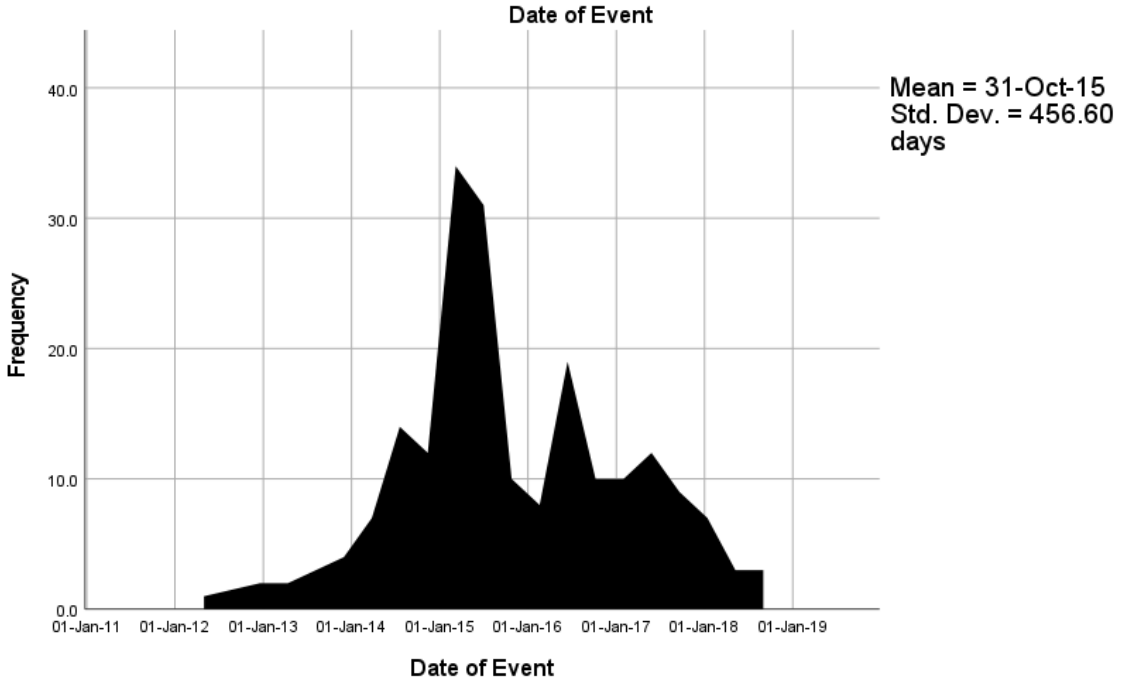


Figure 11 - Date of the Actor's Event

5.3 RQ1: How frequently do terrorists in this sample use the Internet, and in what ways?

The first research question seeks to descriptively explore how terrorists use the Internet. As discussed in Chapter 4, this research derived a codebook from the existing literature (and a round of iterative coding). One of the most important aspects of this is the database research undertaken by Gill and colleagues (Gill and Corner 2015; Gill et al. 2017; Gill 2016; Gill et al. 2015), who demarcate online terrorist activity in two primary ways – whether they have interacted with co-ideologues and whether they have learned about or planned their eventual activity. In turn, these "key" variables are further divided into a range of sub-categories, such as whether the individual disseminated propaganda, supported others, prepared for their event, or overcame hurdles. It was considered worthwhile to replicate the variables used by Gill and colleagues because there are relatively few data-driven studies which disaggregate "online radicalisation" into discrete and observable behaviours. Therefore, a comparison can offer important insights against a dataset from a dataset based in the UK and covering a different time period. This research question also goes beyond merely replicating Gill and colleagues by including several variables not included, such as whether the actor used social media (and which platforms were used), the use of end-to-end encryption, and whether the individual had direct contact with IS.

5.3.1 Online Network Behaviours

For online network behaviours, the key variable is whether the actor had online contact with a wider network, and the sub-variables include using the Internet to reinforce beliefs, disseminate propaganda, supporting others, seeking legitimisation, and recruiting others (Gill et al. 2015), which can be seen below in Table 1, with a comparison to the findings of Gill and others. The data clearly show that online communication of many different types is heavily prevalent within this group of actors. The sample used the Internet heavily to maintain a contact with an online network – almost four in five actors. Of these individuals, the most popular sub-category behaviour was using the Internet to reinforce beliefs, for example by engaging in an ideological discussion with like-minded peers, which over half the sample engaged. Interestingly, there is a sharp increase between each of the behaviours in this sample compared to that of Gill and others, which will be discussed in greater detail below.

Network Behaviour	**Present Study (%)**	**Gill et al (2015; 2017) (%)**
Online Contact with Network	**157 (78.1%)**	**29%**
Reinforce Beliefs	114 (56.7%)	n/s*
Disseminate Propaganda	79 (39.3%)	15%
Support Others	80 (39.8%)	6%
Sought Legitimisation	52 (25.9%)	5%
Recruit Others	53 (23%)	9%

*Not stated in Gill et al. (2015 or 2017)

Table 1 - Online Network Behaviours

It is also appropriate to expand on this work by adding an iterative contribution, coding for several other variables not covered in Gill and others' research. The data show that four in five used social media platforms as part of their antecedent behaviours (expanded on below); as well as over half using social media platforms share their ideology online; slightly under half having direct contact to IS; and around a quarter using end-to-end encrypted platforms (Table 2).

Network Behaviour	Present Study (%)
Contact with IS	98 (48.8%)
End-to-End Encryption	51 (25.4%)
Social Media	163 (81.1%)
Share Ideology Online	112 (55.7%)

Table 2 - Online Network Behaviours 2

5.3.2 Social Media Platforms

As outlined above, 81% of actors used social media for extremist purposes and there was evidence that 56% shared their ideology in an open or semi-open platform, for example, on a Facebook news feed or Twitter timeline.[35] In total, there are 310 instances of individuals using a named social media platform. Figure 12 shows the distribution of the largest social media platforms (used by over 10 actors). Unsurprisingly, the largest platforms such as Facebook (n=96), Twitter (56), and YouTube (51) are represented the most, suggesting that actors gravitate towards the biggest platforms. However, there are several instructive findings: Firstly, despite it being the most popular platform within the sample, fewer than sixty percent of those that used social media used Facebook (and fewer than fifty percent overall). This is lower than the average of all Americans (68%), and even lower than may be expected given that the mean age is 27.5 – the average for the age bracket 25-29 is 80% (Pew Research Center 2018). Secondly, twenty-eight different platforms were identified. Both of these findings suggest a wide social media ecology for terrorists. This is largely in line with research by Conway et al. (2018) who find that disruption of terrorist content by larger social media companies – such as Facebook and Twitter – has led to activity on dozens of different platforms that are more accommodating, sometimes called the "displacement effect".

[35] It is worth noting that sharing ideology on social media is not strictly a network variable because it does not require engagement with co-ideologues, but could simply be outward-only expressions, just as posting on Twitter. However, in the vast majority of cases, it does include communication with a co-ideologue.

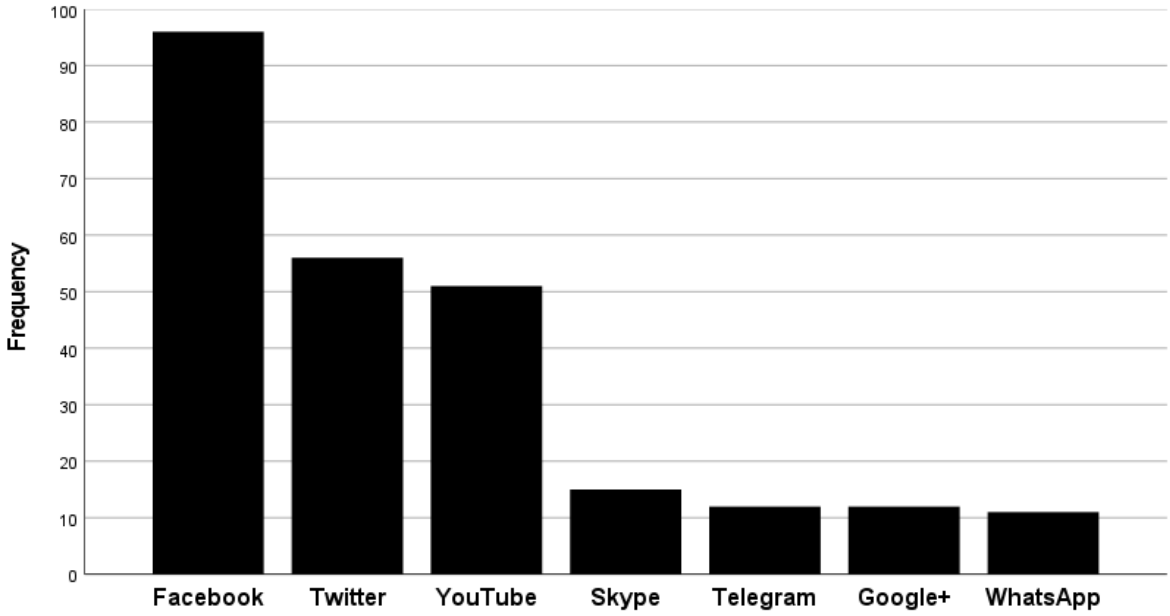


Figure 12 - Social Media Platform used by more than 10 actors

A third instructive finding is the relative lack of end-to-end encrypted social media platforms: Telegram and WhatsApp are used in 12 and 11 instances respectively, a mere 7% of cases in which actors used social media. When adding all the encrypted platforms together, they still only account for a frequency of 36. This is mostly in line with the separate variable for end-to-end encryption, which finds 51 different actors (25%) used end-to-end encryption (note that the former is a frequency of platform use, while the latter is focused on actors' frequencies). The discrepancy between these two numbers can be explained in three different ways:

1. Actors may use multiple end-to-end encrypted platforms;
2. Some uses of end-to-end encryption are not social media platforms (such as using TOR or Bitcoin); and
3. In many cases, the criminal justice information redacts the name of the platform (for example, just says Messaging Platform #1, #2, etc.), but mentions that it is encrypted.

Overall, the relatively low frequency of both end-to-end encryption variables suggests that findings of a widespread "displacement effect" from mainstream platforms towards end-to-end encrypted ones are not supported within this sample, although this will be investigated further using bivariate tests below.

5.3.3 End-to-End Encryption

Given that a sizable minority of the sample use end-to-end encryption, it is worthwhile to explore whether this has increased over time. Previous research has posited a

"displacement effect" from mainstream platforms to encrypted ones, particularly after mainstream social media platforms took a tougher and more proactive approach towards content moderation (Conway 2016b; Reed and Ingram 2019; Bloom et al. 2017). This view has also been reflected by policymakers and law enforcement practitioners, for example former UK Home Secretary Amber Rudd (Lee 2017) and former FBI Director James Comey (McGoogan 2015). However, the descriptive statistics discussed above are not sensitive to the date of the actor's event – i.e. the day of their planned attack, travel, or arrest. It is possible that, as the "displacement theory" suggests, actors mostly used mainstream platforms until around the end of 2015, at which point suspensions drove them away (Berger and Perez 2016; Conway 2016b).

To compare the event dates of the individuals that used end-to-end encryption against those that did not, a one-way analysis of variance (ANOVA) tests was performed. The results indicate that there are no significant differences between the two groups.[36] The distribution can be seen in the bar chart below (Figure 13) and the breakdown of actual and expected figures can be seen in Table 3.

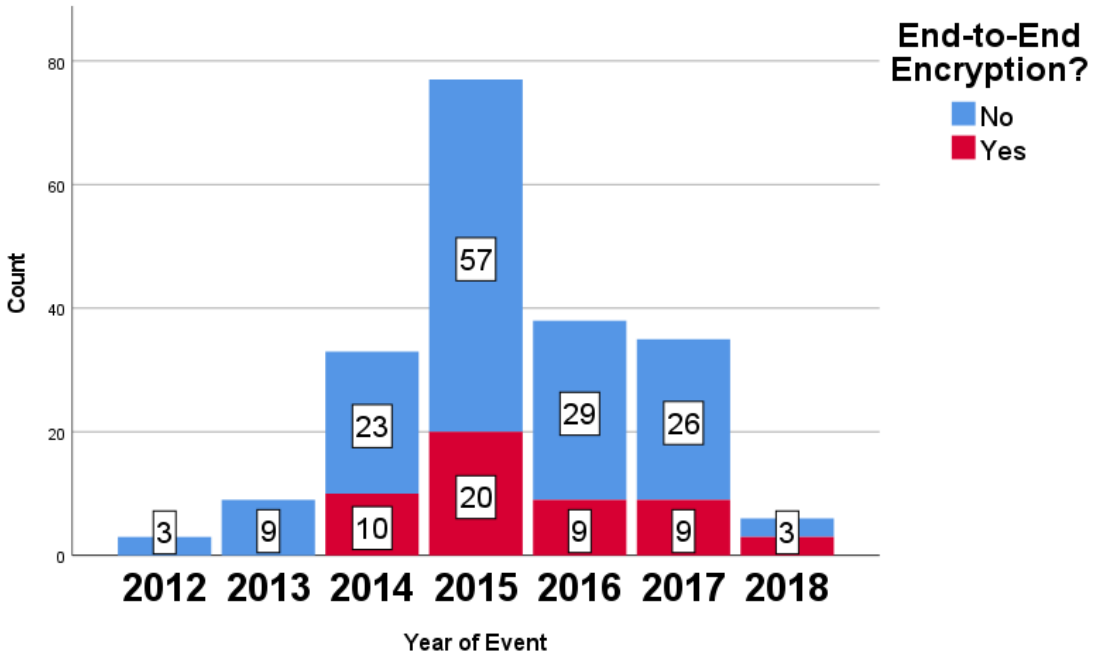


Figure 13 - Year of Terrorist Event by use of End-to-end Encryption

There is no statistically significant increase of end-to-end encryption over time, especially since the end of 2015. Running each individual year as a chi-square analysis shows that the years 2015, 2016, and 2017[37] are all within one integer of their expected count. This suggests that, for this sample at least, the notion of widespread migration away from mainstream platforms may not hold. However, it appears clear from recent research that end-to-end encrypted platforms, particularly Telegram, are central to the jihadist online

[36] $F(1,199) = .741$, $p = .390$.

[37] There were only six new cases in 2018, although end-to-end encryption was used in three of those cases, which is double the expected count.

ecosystem (Bloom et al. 2017; Prucha 2016; Conway and Courtney 2017; Europol 2017; Europol 2018). Recent research has suggested that there are over 600 pro-IS telegram channels that have English-language content (Clifford and Powell 2019). The best way to parse this is to take insight from Gill and Corner (2013) and not to conceptualise all terrorist actors as a homogenous group; in this instance, disaggregating online sympathisers from those that plan and execute attacks may offer an explanation. This goes to the heart of the distinction offered by von Behr et al. (2013) of the "demand" and "supply" sides of researching terrorism online. There are still relatively few studies that analyse the Internet's role in pathways into terrorism. It may be that those that go all the way, rather than merely supporting a group online, have markedly different online behaviours, including the types of social media platform and different levels of interest in online privacy. Similarly, it is also entirely plausible that those that have survived a prolonged online presence are tech-savvy and security conscious, while those in this sample, which is largely made up of those that were caught before a plot was executed, are not.

	No (Expected No)	**Yes (Expected Yes)**	**Total**
2012	2 (2.2)	1 (0.8)	3
2013	9 (6.7)	0 (2.3)	9
2014	23 (24.6)	10 (8.4)	33
2015	57 (57.5)	20 (19.5)	77
2016	29 (28.4)	9 (9.6)	38
2017	26 (26.1)	9 (8.9)	35
2018	3 (4.5)	3 (1.5)	6
Total	150	51	201

Table 3 - Year of Event by Use of End-to-End Encryption

5.3.4 Online Event Behaviours

As with online network behaviours, this research follows the lead of Gill et al. (2017) in establishing several online event behaviours. The results, with a comparison to Gill and others, can be seen in Table 4. As with communicating in an online network, actors used the Internet heavily to learn about or plan their eventual event. In total, almost nine in ten did so online. In particular, they went online to access ideological content (71% - including magazines, memes, and online videos) and preparing for their event (74%), for example, searching for flights online or purchasing firearms.

Event Behaviour	Present Study (%)	Gill et al (2015; 2017) (%)
Learn/Plan Online	178 (88.6%)	54% (76% from 2012-2015)
Access Ideological Content	142 (70.6%)	30%
Online Motivation	43 (21.4%)	14%
Select Target (Attack Only)	17 (32.1%)[38]	9%
Prepare Event	149 (74.1%)	32%
Overcome Hurdles	55 (27.4%)	10%

Table 4 - Online Event Behaviours

Taken together, these findings demonstrate the ubiquity of the Internet amongst antecedent behaviours of terrorists in this sample, which is in keeping with previous research on this topic (Gill et al. 2017; Gill 2016; Bastug, Douai, and Akca 2018; von Behr et al. 2013). In total, only 19 case studies (9.5%) did not demonstrate evidence of either network activity or learning/planning their event via the Internet. Moreover, this research question also demonstrates the wide array of different activities that the terrorists in this sample engaged in online. Ideological conversations and learning were popular across both sets of sub-variables, such as accessing and disseminating propaganda, as well as developing a motivation to act. However, actors also went online for facilitative behaviours, such as target selection, preparing events, recruiting and supporting others, and overcoming hurdles. This wide range of behaviours is also reflected in the variety of different social media platforms; rather than sticking to one site with specific affordances and architecture.

5.3.5 Increase in Internet Usage

As well as terrorists using the Internet ubiquitously, a comparison of this sample to the research of Gill et al. (2017) demonstrates that there seems to be a sizable increase in

[38] Valid percentage of the 55 attackers.

online antecedent behaviours, potentially suggesting a greater reliance on the Internet. Below, I offer four potential explanations as to why the Internet appears more prominently in both network and event behaviours:

The first and most intuitive explanation is that in recent years, Internet usage has increased. Gill and others' studies include cases of terrorism that date back to 1995 through to 2015. In that time, global use of the Internet went from 0.4% to 46% (Internet World Stats 2019). It makes intuitive sense that as usage increases among all users, it too increases with terrorists. This point is highlighted by Gill and others, who observe that 54% of actors use the Internet to learn or plan their event, but when this is narrowed to the period 2012-2015, that number rises to 76%, suggesting that the early cases weigh the number down. In research on US-based extremists by Jensen, James, et al. (2018) find a steady increase in social media usage from 2005 (8%) to 2016 (87%). When considering an US-based sample from 2012-2018, (i.e. both this research and that of Jensen, James, and colleagues) it is instructive to note that total Internet usage has increased from around 52% in 2000 up to 89% in 2018 (Pew Research Center 2019) (Figure 14) – the same number as learned about or planned their attack online. This increase seems to represent an increase that is congruous with the findings of Gill and others. In short, the Internet has become ubiquitous and terrorists have merely followed this trend.

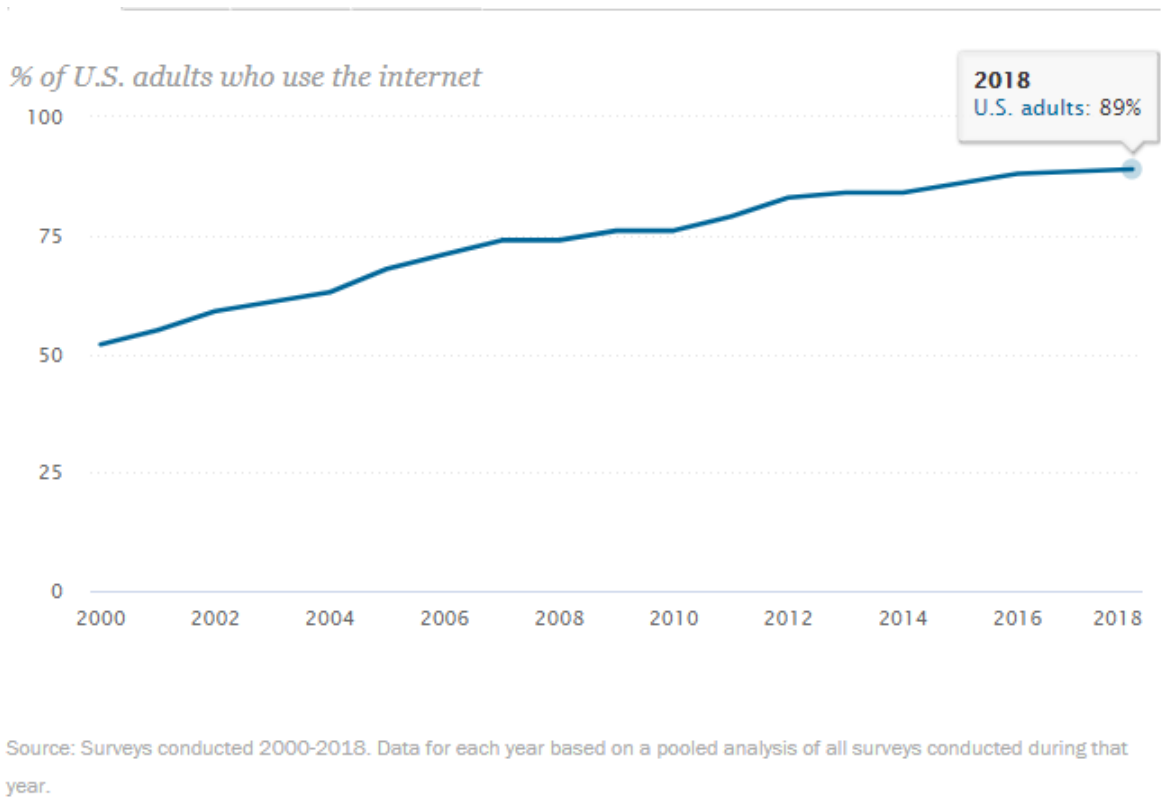


Figure 14 - US Adults' Internet Usage (Pew Research)

A second explanation is that, due to differences in criminal justice privacy norms between the US and the UK, the sources in this research are different to Gill and others. The former

utilises criminal justice documents as well as news reports, while the latter uses mostly news reports because court documents are more difficult to come by without access to closed-source data in the UK (Gill et al. 2015). As explained in Chapter 4, these sources provide different types of data, with the criminal justice documents providing rich, granular data and often described the antecedent online behaviours – such as Google search history or the actor's Twitter posting history – in great detail – these documents are often hundreds of pages long. In contrast, news reports tended to focus on interviews with friends and family and it may not fit editorial guidelines to report on such granular data points. Support for this can be found in other research by Gill (2016) where he analyses closed-source police data over the period 1995-2015 and finds much higher use of the Internet (59% for online network and 82% for online learning/planning).[39] The police data in Gill's study were far more granular and rich, including 'information contained in police data files, psychological reports (when available), interviews with case officers, intelligence reports, and open-sources for further context within each case' (Gill 2016, pp.2–3). This would suggest that the method of data collection matters a great deal. However, the Gill et al. (2015) study remain the best comparison for this research because the 2016 study only offers a small number of variables and no bivariate analysis.

Behaviour	**Gill et al. (2015; 2017) – Open Source – 1995-2015**	**Gill (2016) – Closed Source – 1995-2015**
Online Network Interaction	29%	59%
Learn/Plan Online	54% (76% from 2012-2015)	82%

Table 5 - Open versus Closed-Source Data

The third explanation is that there may be geo-social reasons for the difference in Internet use among terrorist actors. In general, the academic literature suggests that offline social networks play a more important role than the Internet in trajectories towards terrorism (von Behr et al. 2013; Gill et al. 2017; Reynolds and Hafez 2017; Vidino et al. 2017). However, it is possible that America may be anomalous to this trend; in their report discussing the flow of foreign fighters to Iraq and Syria, The Soufan Group note that around the world, recruitment hotspots (i.e. offline social networks) best explain travel, but within the United States social media plays a particularly important role, especially in the initial phases of the process. Importantly, they note that: 'There are no significant

[39] It is worth noting that this study was based solely on lone actors so cannot be seen as a direct comparison, particularly because Gill et al. (2015; 2017) find that lone actors are more likely to use the Internet than group-based ones. However, it is still very likely that the type of data can substantially affect findings.

patterns of locally based recruitment in the Americas — nor recruitment hot spots[40] — as seen in Europe and the former Soviet republics' (Soufan Group 2015, p.20). Similarly, Vidino and Hughes note that 'Social media plays a crucial role in the radicalization and, at times, mobilization of U.S.-based ISIS sympathizers' (Vidino and Hughes 2015, p.ix), although they do highlight the importance of offline interactions too. Taken together, it is worth considering that there may be geo-social explanations for the difference between the British online behaviours studies by Gill and others and in this study: the touted lack of robust offline social networks in the US shifts the burden onto the Internet.

Finally, as discussed in Chapter 4, it must be reiterated that this project was undertaken independently to that of Gill and colleagues. While every effort was taken to ensure rigour in coding, it is possible that there are subjective differences that emerge between the two studies. For the key variables, this should be minimal because there is little room for interpretation when assessing whether an actor interacted with ideologues or not, or whether they used the Internet to learn about their event. However, some of the sub-variables, such as whether the actor reinforced their beliefs online or were motivated by something they saw online could leave more room for subjective differences between coders.

It may be tempting to interpret a rise in Internet usage among terrorist actors as a direct result of an increase in usage among the general population because it follows a simple, mono-causal explanation. However, for the reasons outlined above, there may be several other factors at play that increase the numbers.

5.4 RQ2: Has the Internet replaced the offline domain as the primary venue for terrorists' antecedent behaviours?

RQ1 demonstrated that terrorists used the Internet heavily as part of their trajectory, engaging in a range of different behaviours. At first glance, one may draw the conclusion – similar to that of Sageman (2008b) – that the online domain is becoming the primary avenue in pathways towards terrorism, which may be an indicator that online radicalisation is prevalent within contemporary terrorist populations. However, to make such an assessment, one must compare the online behaviours outlined above to offline ones.

To do this I follow the lead of Gill and others who conduct a series of Pearson's chi square tests, and Fisher's exact tests (Gill et al. 2017). Both test the frequencies that two events occur for the same actor against the frequencies that may be expected given a random distribution. If the difference between the frequency and the expected frequency is significantly different (demonstrated by a p value of <0.05 – which suggests a less than

[40] This report may have been written too early to identify what can only be described as a recruitment hot spot in Minneapolis, MN metropolitan area as many of the actors were charged in 2015.

5% probability the results could have occurred by chance), then the null-hypothesis – that the variables are independent – can be rejected. One of the assumptions of a chi-square test is that each of the possible outcomes has an expected frequency of five, therefore, in instances in which that is not the case, Fisher's exact test is utilised, which overcomes small sample sizes by calculating the exact probabilities of each potential outcome (Field 2018).

To establish whether the Internet has become the primary venue for radicalisation by testing whether online behaviours are correlated to offline ones. If there is a strong positive correlation between the two domains, it suggests that individuals who act in one domain tend to also act in the other. If there is no relationship and actors are acting primarily in the online domain, but not offline, then one could plausibly make an argument for "online radicalisation."

What follows below is the descriptive statistics for two of the variables of interest: engaging in an *offline* network and learning or planning *offline*. These will then be tested against the online behaviours presented in the previous RQ as the results of the chi-square (and Fisher's exact where appropriate) analyses that relate to different online behaviours are presented, reporting the x^2 value (obtained by adding each of the standard deviations together); the *p* value (which reports the significance); the percentage of the total sample that make up the relationship; and the odds ratio, which expresses how big the observed differences are in instances with four possible outcomes by multiplying the instances in which both variables are present by instances in which neither are present, then dividing by the instances in which one is present (Field 2018). For example, interacting in an online network has two outcomes (Yes/No), and learning/planning offline has two (Yes/No). The odds ratio multiplies those that both engaged online *and* those that learned/planned offline by those that did neither, before dividing by the cases where only one of the two instances are observed (i.e. A x D/B x C).

5.4.1 Offline Behaviours - Descriptive

Before conducting the bivariate analysis, it is worthwhile to present the descriptive statistics of two variables which will be tested against online behaviours. These are the converse of the online "key variables" – 1) maintaining contact with an offline network and 2) learning about or planning an event offline:

Behaviour	***Frequency***
Offline Contact with Network	138 (68.7%)
Learn/Plan Offline	150 (74.6%)

Table 6 - Offline Behaviours

Although the terrorists in this sample used the Internet heavily in the run-up to their events for variables behaviours – as established in the previous RQ – these descriptive statistics suggest that their antecedent behaviours also spilled over into the offline domain. There were several cells that maintained an offline network of like-minded

peers, such as the cluster of around 20 individuals who attempted to travel in various waves from the Minneapolis/St Paul region of Minnesota;[41] a group of individuals in the New York/New Jersey area;[42] and those involved in the attack in Garland, TX on May 3, 2015.[43] Similarly, individuals prepared for their events offline by scouting out targets, such as Matin Azizi-Yarand, who plotted an attack on a shopping mall in Texas, but conducted recognisance beforehand,[44] or Asia Siddiqui and Noelle Velentzas, who attempted to construct a bomb to use as part of an attack.[45]

5.4.2 Online Network Behaviours versus Offline

Next, to establish whether the online domain is replacing the offline, I test the relationship between those that engaged in an online network – both the key variable and the sub-variables – against those that engaged in an offline one. Those that engaged in an online network were 3.63 times more likely to engage in an offline network as well. That is to say, despite high usage, the Internet does not seem to be replacing the offline domain as the primary path towards terrorism; rather, actors tend to communicate in both spheres. This is further exemplified by four further significant correlates between each of the following variables and engaging in an offline network: using the Internet to reinforce beliefs, supporting others, contacting IS, and seeking legitimisation – these results can be seen in Table 7. This is congruous with the findings of Gill and others, who find that 'those who communicated online were 3.89 times more likely to have experienced nonvirtual network activity' (Gill et al. 2017, p. 111). Take, for example, Mahmoud Amin Mohamed Elhassan, who maintained an offline relationship with Joseph Hassan Farrokh and facilitated the latter's travel to Syria. At the same time, he had an active voice in the jihadist Twitterverse and maintained a relationship with radical Sudanese cleric Mohammed Ali al Jazouly.[46] This is a relatively typical example – while expressing one's views as part of an online community has become commonplace, it does not seem to supplant the importance of offline interactions in trajectories towards terrorism.

[41] USA v. Mohamed Abdihamid Farah et al. Criminal Complaint.
[42] USA v. Samuel Topaz, Criminal Complaint, [Unknown Case #] United States District Court for the District of New Jersey, 2015. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Topaz%20Criminal%20Complaint.pdf.
[43] USA v. Abdul Malik Abdul Kareem, Government Sentencing Memorandum, Case 2:15-cr-00707-SRB, United States District Court for District of Arizona, 2016.
[44] USA v. Matin Azizi-Yarand, Affidavit for Arrest Warrant, Case Number: 18045858, Warrant Number: 18-136, State of Texas, Warren County, 2018.
[45] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint, Case 1:15-mj-00303-VVP, United States District Court for the Eastern District of New York, 2015.
[46] USA v. Mahmoud Amin Mohamed Elhassan, Government Sentencing Memorandum, Case 1:16-cr-00064-AJT, United States District Court for the Eastern District of Virginia, 2017.

	Offline Network			
Behaviour	**x^2 Value**	***p* Value (Sig.)**	**%**	**Odds Ratio**
Online Contact with Network	14.092	.000	85.5	3.631
Reinforce Beliefs	5.629	.013	62.3	2.067
Support Others	6.291	.009	45.7	2.273
Contact IS	4.174	.029	53.6	1.879
Seek Legitimisation	3.384	.046	29.7	1.998

Table 7 - Offline Network and Online Network Behaviours Significant Correlates

5.4.3 Online Learning/Planning Behaviours versus Offline

As with offline networks, the data show those that plan their event in the online domain are significantly – 4.79 times – more likely to also learn or plan offline too. This, again, is in line with the findings of Gill and others, for whom offline learning was 3.17 times more likely to be accompanied by online (Gill et al. 2017). Omar Mateen, the Pulse nightclub shooter, conducted both physical surveillance by driving around Orlando eight days before the attack observing numerous clubs,[47] as well as online learning by Googling "downtown orlando nightclubs" in the minutes prior to the attack.[48] Despite the incredible growth in the ability to discern information online, actors are considerably more likely to be acting in both domains. There was also a significant correlation between offline learning and planning and communicating with co-ideologues online, which actors were 2.28 times more likely to be doing; Gill and others observe that actors were three times more likely too (Gill et al. 2017). The only online learning/planning sub-variable which held a significant correlation with offline learning and planning was the selection

[47] USA v. Noor Salman, Government's Motion for an Order Revoking Defendant's Release, Case 6:17-cr-00018-PGB-KRS, United States District Court for the Middle District of Florida, Orlando Division, 2017.
[48] USA v. Noor Salman, Defendant's Motion to Preclude Improper Argument in Government's Opening Statement, Case 6:17-cr-00018-PGB-KRS, United States District Court for the Middle District of Florida, Orlando Division, 2018.

of an attack target online, for example, Omar Mateen. This suggests that it is a collection, rather than a single sub-variable that drives this relationship.

Importantly, there are no significant correlates between learning or planning online (including the sub-variables) and engaging in an offline network, which marks a departure from Gill and others, who find that 'Those who learned online were 4.39 times more likely to have experienced nonvirtual network activity' (Gill et al. 2017, p.12). This, of course, does not mean that offline communication is less likely, but rather that the frequencies fall close to their expected counts.

	Offline Learning/Planning			
Behaviour	**x^2 Value**	***p Value (Sig.)***	**%**	**Odds Ratio**
Learn/Plan Online	13.308	.001	93.3	4.789
Select Target Online (Attack Only)	4.449	.034	37.8	.778
Online Contact with Network	5.233	.020	82	2.278

Table 8 - Learning and Planning Offline and Learning and Planning Online Significant Correlates

Looking at the relationship between the two key variables – engaging in an online network and learning or planning online – and each of their offline counterparts, there is an observable pattern that is parallel to the findings of Gill et al. (2015). Simply put, despite Internet use being prevalent, the offline domain seems, at the very least, equally important. These results suggest that instances of a terrorist actor radicalising via only online interactions are still relatively rare. Rather, the Internet facilitates, rather than replaces, offline interactions and planning. This also goes somewhat against the idea – posited above – that America may be exceptional with regards to a greater reliance on social media. The data suggest that terrorists are still acting in both domains.

5.5 RQ3: Do terrorists that use the Internet exhibit different experiences to those that do not?

Although RQ2 demonstrated that the Internet does not appear to be replacing the offline domain as the primary venue for radicalisation – as suggested by scholars like Sageman (2008b) – the next logical question is whether engaging on the Internet offers affordances that lead to different user experiences. For example, Gill and colleagues (2017) find that

lone actors are significantly more likely to learn via the Internet than their group-based counterparts, who can pool human, social, technical, and financial capital.

This RQ will first present the descriptive statistics for the variables of interest that are related to actors' events, such as the four categories assigned to the number of actors that execute a plot; the role that actors had in events; for those that attack, the type and target of the attack, as well as whether it was deadly. Then, these event behaviours and other demographic variables, such as age and gender, will be tested against the online behaviours discussed above to assess whether those that use the Internet are more likely have different experiences than those that do not.

5.5.1 Event Behaviours – Descriptive

Actors and Co-offenders

To discern the number of offenders involved in the execution of a plot, this RQ divides individuals into the categories used by Corner, Gill, and Mason (2016):

1. Lone actors – execute the plot alone without direction from a group;
2. Solo actors – execute the plot alone but with direction or support from a wider network;
3. Lone dyads – two actors that execute the plot together; and or
4. Group actors – for any number of actors above two executing the plot.

There is a relatively even split between these four categories, with lone actors and solo actors encompassing around a quarter of the sample each, lone dyads around one-fifth, and group actors one third (Figure 15). Horgan et al. (2016) find that around a fifth of their sample could be considered lone actors, with the other four-fifths acting in a group – not delineating between the other three categories.

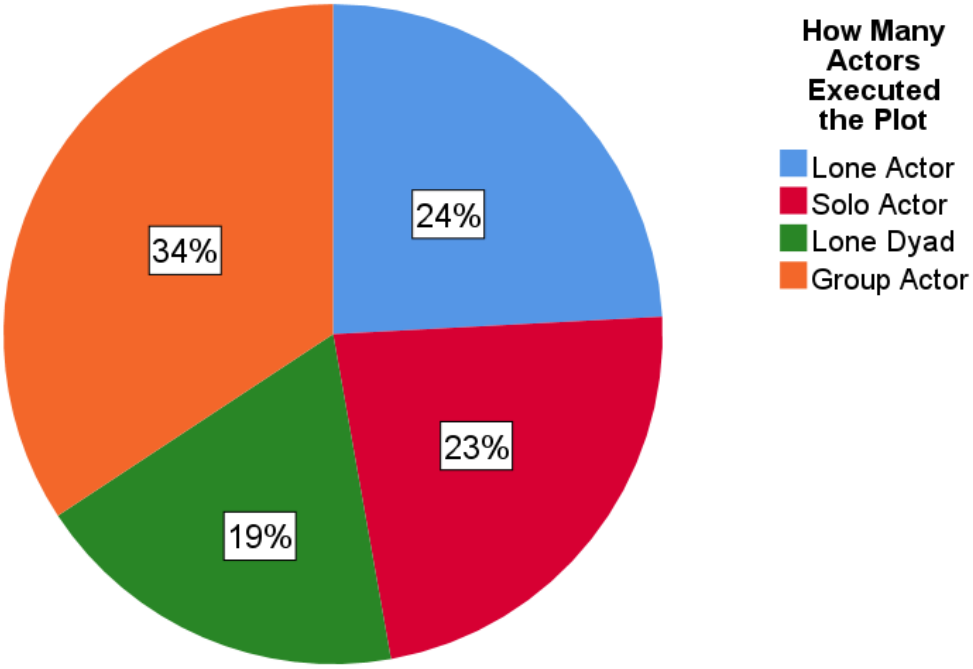


Figure 15 - Number of Actors Involved in Execution of the Plot

There are two noteworthy points to make regarding these descriptive findings. Firstly, the argument offered by Schuurman et al. (2017) on the problematic nature of labelling someone a true "lone" actor (i.e. no contact with any other actors as part of their trajectory or plot) is apparent when looking at this data. There are 24 cases (12%) of actors that had no online or offline contact with a network, but many of those cases can be attributed to a lack of data. For example, Mohimanul Bhuiya is not explicitly mentioned to have engaged in either an online or offline network, even though it is stated that his unspecified "online activity" caused the FBI to visit him and he successfully travelled to Syria.[49] Given the difficulty in travelling to the caliphate without any assistance (most actors utilise contacts within IS as a reference as well as smugglers at one of the Turkish border towns), it seems implausible that he did not have contact with an online network. It is far more likely that he fits the role of a solo actor than lone. This is a limitation to open-source data, but it is important to both be precise and not to over-interpret the number of lone actors. The vast majority are communicating (or are very likely to be communicating) as part of a wider network. There are, however, some actors such as Edward Archer that do not appear to have been in contact with a wider network and may fit the definition of a "true" lone actor.[50]

Secondly, the US may present a further complication because of the high prevalence of undercover sources or officers. Previous research has found that the US security services

[49] USA v. Mohimanul Bhuiya, Criminal Complaint, Case 1:14-cr-00612-JBW-RLM, United States District Court for the Eastern District of New York, 2014.
[50] Associated Press, Man Accused of Shooting Philly Officer Convicted of Attempted Murder, *ABC News*, Febuary 1, 2018, http://6abc.com/man-accused-of-shooting-philly-officer-found-guilty/3018942/.

rely heavily on undercover agents as part of terror investigations and prosecutions (Horgan et al. 2016; Human Rights Watch 2014; Greenberg and Weiner 2017). With regards to the number of actors executing a plot, this leaves two methods of coding. One can code for the number of "true" extremist actors, or code for the individuals that an actor *believes* they are interacting with. Ultimately, it is deemed that the latter offers a fuller understanding of individual trajectories and group dynamics. However, it could be argued that it skews this variable, creating several group actors that may otherwise have acted alone (or not acted at all[51]). In other jurisdictions, lone actors may have no choice but to act alone because they are unable to forge and maintain inter-personal relationships (Corner et al. 2018), but in the US, artificial relationships can be created by law enforcement in which an actor's inability to maintain social relationships is tolerated by the undercover agents. Given this US specific issue, it is important to note that the dynamics of individual trajectories may differ to other parts of the world.

Disaggregating the role of a "Terrorist"

It is prudent to disaggregate the different roles involved in being a terrorist; Corner, Gill, and Mason (2016) note that many studies have aggregated the notion in a generic fashion. The experience and behaviours of attackers may be different to that of financiers, which may be different to that of bomb-makers; 'their roles, functions, expectations, and experiences may differ in terms of recruitment, (self-) selection, [and] routine activities while "being" a terrorist' (Corner, Gill, and Mason 2016, p.560). To that end, five categories are utilised to demarcate the potential or eventual role in the event: Attacker, traveller, financier, facilitator, and bomb-maker, which are outlined below in Table 9. It is worth noting that the number of cases adds up to more than 201 because it is a multiple response set; that is to say, an actor can be an attacker and a bomb-maker, like Everitt Aaron Jameson, who sought to attack Pier 39 in San Francisco and also attempted to acquire materials to make a bomb to do it.[52] Despite the image of a terrorist often being viewed as that of an attacker, they make up a relatively small number of incidents (n=55). Rather, this sample is more defined by the 97 travellers – just under half of the whole database, perhaps reflecting IS' aims at state-building in their propaganda, as discussed in Chapter 3. These categories can be utilised to assess whether the online behaviours of different terrorist actors are fundamentally different to each other.

[51] Human Rights Watch (2014) argue that the excessive use of undercover officers created terrorists out of law abiding citizens that would have been unlikely to break the law had they not been assisted by the FBI.
[52] USA v. Everitt Aaron Jameson, Criminal Complaint, Case 1:17-mj-00225, United States District Court for the Eastern District of California, 2017.

Role	Frequency:	Percent (%)	Percent of Cases (%)
Attacker	55	22%	28.2%
Traveller	97	38.8%	49.7%
Financier	39	15.6%	20.%
Facilitator	43	17.2%	22.1%
Bomb-maker	16	6.4%	8.2%
Total	250	100%	128.2%

Table 9 - Actor's Role in Event

Attack Behaviours

The 55 identified attackers are further disaggregated below. Firstly, the type of attack is split up into four categories: Armed assault (n=33); unarmed assault (11); IED attack (25), and vehicle-based attack (3). It is again worth noting that this is a multiple response set and therefore the frequencies add up to more than 55, as actors can fulfil multiple criteria, like the San Bernardino bombers Rizwan Farook and Tashfeen Malik, who attempted to detonate pipe bombs as well as conducting an armed assault.[53] The prevalence towards armed assault is intuitive given the constitutional protection given to Americans under the Second Amendment. IS repeatedly offered operational advice to recruits to conduct attacks in the simplest way possible, including a famous speech from official spokesman Abu Mohammad al-Adnani, who said:

> Kill him in any manner or way however it may be. Smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him. (Al-Adnani 2018)

While in other countries this manifested in vehicle-born attacks, access to firearms is so widespread in America that an armed assault remains a simple method of attack that can inflict a high number of casualties.

[53] Megan Christie et al., Christmas Party May Have Triggered San Bernardino Terror Attack: Police.

The target of the attack is also categorised in four ways: Government (n=5), civilian (34), military (2), and police (7).[54] This, perhaps, again speaks to conducting the simplest attack possible as civilian targets are likely to be ones that require the least planning and meet the least resistance. Of the 55 attacks, only eight (15%) resulted in a fatality, which may highlight the downside of planning attacks around simplicity and speed.

5.5.2 Online Network Behaviours versus Event Behaviours

Having tested the key variables and their subsequent sub-variables against their offline equivalent, it is important to assess whether those that do use the Internet as part of their trajectory exhibit similar behaviours to those that do not.

With regards to the roles in the event, only facilitators and financiers have a significant positive relationship with engaging in an online network. This again makes sense as both facilitating and financing events requires some kind of communication with another actor, although when running crosstabs for engaging in an *offline* network versus role in an event, only facilitating held a significant correlation. Those that conducted an IED attack were 4.02 times more likely to communicate online, which also mirrors a finding of Gill et al. (2017), as one may expect the difficulties involved in participating in such an attack may require coordination of some kind. There are no significant correlates for any attack target type.

	Online Network			
	***x*² Value**	***p Value (Sig.)***	**%**	**Odds Ratio**
Recruit Others Offline	10.719	.000	34.4	5.243
Attacker	3.602	.046	24.2	.507
Financier	5.705	.010	22.9	4.066
Facilitator	9.508	.001	26.1	7.422
IED Attack	4.771	.028	55.3	4.015

Table 10 - Online Network and Event Behaviours Significant Correlates

[54] This variable is also multi-entry and the combined totals add up to only 48, given that a number of attacks were thwarted at the planning stage without a target being fully chosen.

5.5.3 Online Learning/Planning Behaviours versus Event Behaviours

It is prudent to assess whether those that used the Internet to learn about or plan their activity exhibited markedly different behaviours from those that did not. Interestingly, none of the following variables were positively related to online learning or planning: the role in event, and type of attack or target. Gill and others find a correlation in each of these categories. Take for example, learning or planning versus conducting an IED attack:

> Of all those who actually plotted an attack, those who used/planned to use an IED were 3.34 times more likely to have learned online. This reflects both the greater complexity in IED manufacturing compared with other weapons coupled with the relative ease of availability of online bomb-making manuals and YouTube videos that provide helpful demonstrations. On the other hand, those who used more primitive attack types, like arson or unarmed assaults, were significantly less likely to have learned online (Gill et al. 2017, p.12)

Within this sample, IED attacks are not positively correlated and more "primitive" attacks – unarmed assault, armed assault (given the aforementioned ease in obtaining firearms), or vehicle-based assault – are not negatively correlated. Given that Gill and others' findings make logical sense, this is an interesting finding that is presented without an obvious explanation.

5.5.4 Number of Co-offenders versus Online Behaviours

Just as it is important to disaggregate the type of terrorist actor when analysing descriptive statistics, it is also worthwhile to compare the differing number of actors involved in the execution of the plot against online learning/planning behaviours. One might expect an inverse relationship between the number of actors and using the Internet to learn about or plan their event. That is to say, supplementing the lack of other actors involved in a plot that can provide operational support and advice with online resources. Gill and others find exactly this: lone actors were 2.64 times more likely to learn online than members of a cell (Gill et al. 2015).

Because the coding variable for the number of co-offenders was a four-answer multiple-response (i.e. "lone actor," "solo actor," "lone dyad," "group actor"), conducting a chi-square analysis is inappropriate as it requires variables with two outcomes each to produce an odds ratio. Therefore, each of these responses were converted into binary dummy variables and then were each tested against learning/planning online.

Interestingly, there does not seem to be a particularly strong relationship between learning and planning online and the eventual number of co-offenders in a plot. Lone actors were no more likely to use the Internet for planning than other sized plots – this runs country to both Gill and colleagues as outlined above as well logic. It is worth noting that there was evidence that the vast majority (84%) of lone actors did use the Internet (36 out of 43), but that is roughly in keeping with the rest of the sample.

There is a significant relationship between solo actors and learning/planning online (x^2 = 4.121, p = 0.029, 97.6%, OR = 6.377), potentially suggesting that their command-and-control links may have involved online learning, like in the case of Reza Niknejad, who despite travelling to the caliphate alone, aided online by both Ali Shukri Amin and unnamed co-conspirators from within IS territory, who helped him prepare for his travel and evade suspicions.[55] There are no significant correlates for either lone dyads or group actors; both categories used the Internet heavily (91% and 87% respectively), which is in keeping with the wider sample.

Bivariate analyses for engagement in an online or offline network and the number of actors are not offered because it violates the assumption of independence for chi-square tests – i.e. it is built in that solo actors, lone dyads, and group actors will engage in an network because they are part of a network by definition. However, an instructive finding is that there was evidence that eighteen of the 43 (42%) lone actors *did* have contact with a wider online network. Although this is less than one would expect given a random distribution, it still speaks to the arguments made by Schuurman et al., that despite executing a plot alone, many lone actors still have 'ties to both online and offline radical milieus [which aids] the adoption and maintenance of both the motive and capability to commit acts of terrorism' (Schuurman et al. 2017, p.1). That is to say, lone actors are often not truly alone. Take Joshua Ray van Haften, who disappeared from Chicago alone in 2014 for Istanbul with the intention of crossing the border to Turkey. However, at his trial it emerged that he was a frequent poster on different social media platforms within the online milieu and even offered operational advice to Leon Davis, who was also charged with attempting to join IS.[56]

5.5.5 Age versus Online Behaviours

It is a longstanding cultural meme that younger people are more likely to be at the forefront of technology than their elders, which one might expect to translate to Internet usage. This idea traces at least as far back as 2001 with Prensky's famous demarcation between "digital natives" and "digital immigrants". He argues that young people are better placed to navigate digital surroundings if they are similar to the environment in which they grew up (Prensky 2001). This may suggest that younger terrorist actors may be more likely to use the Internet compared to the older members of this sample. There is good reason to think that this may be the case; one of the key findings of Gill and Corner's work on lone actors in the UK and the US is that younger offenders are significantly more likely than older ones to both learn/plan their events online and engage in an online network (Gill and Corner 2015). This seems to follow the idea that youth may be an indicator of using the Internet to engage in terrorism.

[55] USA v. Ali Shukri Amin, Statement of Facts, Case 1:15-cr-00164-CMH, United States District Court for the Eastern District of Virginia, 2015.

[56] USA v. Joshua Ray van Haften, Government Sentencing Memorandum, Case: 3:15-cr-00037-jdp, United States District Court for the Western District of Wisconsin, 2017.

ANOVA tests were performed to assess the average ages of the individuals that used the Internet compared to those that did not. The first ANOVA tested individuals' age against the variable of maintaining contact with a network, finding there to be no significant relationship.[57] Similarly, the second ANOVA, which analysed the ages of individuals that learned or planned online against those that did also found not significant correlates.[58] In both cases, individuals that acted online were not more likely to be younger than those that did not, as one might expect if they extrapolated Prensky's argument.

This suggests that age is not a particularly reliable indicator of using the Internet as part of involvement in terrorism. When looking at general population data, there may be some support for this; within the US, the age groups 18-29 and 30-49 have a 98% usage of the Internet, while 50-64 use it 87% of the time, and 65+ have a 66% usage (Pew Research Center 2017b). Given that there are no actors in the sample above the age of 65, the data suggest that today, for every age group that is represented in this database, the Internet is ubiquitous for almost everyone – which might lead one to question why terrorists would be any different. It seems that the most likely explanation for the departure from the findings of Gill and Corner is that the sample in their study dates back to 1990 and at various periods there have been considerably bigger gaps between the age groups,[59] with younger people using the Internet disproportionately more.

5.5.6 Gender versus Online Behaviours

The tripartite relationship of the Internet, terrorism, and gender is an important and understudied one, particularly in the context of jihadism. While in general, scholars have focused on the importance of offline interactions in trajectories towards terrorism (Gill et al. 2015; von Behr et al. 2013; Reynolds and Hafez 2017), studies focusing specifically on gender have highlighted that the Internet may offer a different experience in which females have a greater degree of freedom to explore the radical milieu than they might have in the offline domain (Huey and Witmer 2016; Pearson 2016; Bermingham et al. 2009).

However, when gender is tested against the online network and event variables, no significant correlates are found – suggesting that the 20 women in this sample are not more likely to rely on the online domain than their male counterparts. This does not mean that there are no gender dynamics at play, but rather they are complex and may not be captured by coding dichotomous variables. Therefore, gender dynamics in the online realm will be discussed in Chapter 6.

[57] $F(1,195) = 1.488$, $p = .224$
[58] $F(1,195) = .290$ $p = .591$
[59] For example, in 2009, Internet usage was as follows: 18-29 (92%); 30-49 (84%); 50-64 (75%); 65+ (40%). In 2000 it was: 18-29 (70%); 30-49 (61%); 50-64 (46%); 65+ (14%). (Pew Research 2019)

5.6 RQ4: Does using the Internet help or hinder plots?

One might expect, given discussions of "online radicalisation", that the Internet poses a menace to society by affording would-be terrorists both the ideological affinity and operational knowhow to successfully conduct attacks. However, this is not necessarily the case. In a study of US-based extremists conducted by Jensen, James, et al (2018), they find that terrorists that were active on social media were less likely to be successful than those who were not. Similarly, Gill and Corner (2015) offer this analysis in their study on the online behaviours of British lone actor terrorists:

> Despite the many benefits of virtual learning and virtual activity described above, the individuals who interacted virtually with co-ideologues were significantly less likely to actually carry out a violent attack. Indeed, the individuals who learned through virtual sources were also significantly less likely to kill or injure anybody. This is all the more surprising when we consider the fact that they were significantly more likely to plot an attack against indiscriminate soft targets. (Gill and Corner 2015, p.49)

Gill and Corner find it surprising that the Internet may be an impediment to success, given it can offer the ability to download bomb-making materials within a few short clicks or receive operational advice from experts, such as the virtual entrepreneurs of IS, who from Raqqa, directed actors to commit a number of attacks in the US and around the world (Hughes and Meleagrou-Hitchens 2017).

To test this, four event or post-event behaviours are tested against online behaviours, including those that could be construed as success (or failure) on the part of the actor, such as whether the event was successful; whether the actor was known to the security services prior to the event; whether the actor was arrested. The descriptive statistics for each of these variables are presented immediately below, followed by chi-square analyses of both the main online variables (online contact with a network and learning/planning online) and their subsequent sub-variables. Given the sizable number of strong correlations, the analysis uses a binary logistic regression to establish whether one behaviour predicts event success.

5.6.1 Post Event – Descriptive

Only a relatively small number – 40% – of the total events were successful, with the majority being halted before the plot could be executed. 157 (78%) of the database were arrested for their activity. As discussed above, the US relies heavily on undercover agents as part of their counter-terrorism investigations (Horgan et al. 2016; Human Rights Watch 2014; Greenberg and Weiner 2017). In this sample an undercover agent was used in 43% of cases, however, in cases in which the actor was arrested, this number increases

to 61%. Of the 163 criminal charges,[60] 57 (35%) are still awaiting trial,[61] 89 (55%) pleaded guilty, while 17 (10%) went to trial and were found guilty. Only one actor connected to IS has been acquitted at trial - Noor Salman, the wife of Pulse Nightclub shooter Omar Mateen. She was removed from this sample because she was not deemed to self-identify with the group. Each of the average sentences is ten years or over, with a mean of 184.7 months; a median of 144 months; and a modal value of 120 months.[62] A polygon of the sentence by frequency can be observed in Figure 16.

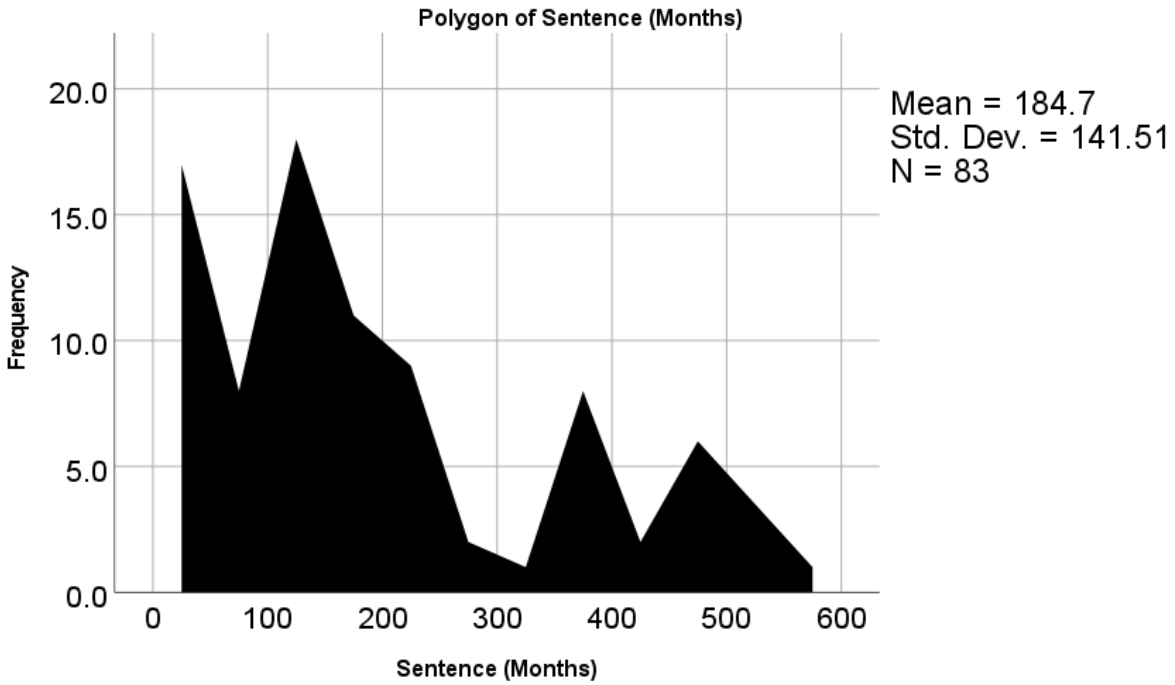


Figure 16- Length of Sentence

5.6.2 Post-Event Behaviours versus Online Activity

To establish whether online behaviours were indicative of success, the two variables of online learning and planning were tested against the dichotomous variable of whether the event was successful. These were tested against the two key variables and each of their respective sub-variables. As Table 11 demonstrates, online behaviours demonstrate a range of significant inverse correlations with the success of events. Individuals that used the Internet to maintain contact with a network were only a quarter as likely to be successful as those that did not, and those that learned or planned were only a one-seventh as likely to be successful. Moreover, rather than a single behaviour, eight sub-variables were also significantly inversely correlated. This lends weight to the notion that

[60] The reason for the discrepancy between arrests (157) and actors charged (163) is that a small number, such as Abdi Nur – a Minnesotan successful traveller – were charged in absentia without being arrested.
[61] As of the end of December 2018.
[62] I follow the lead of the George Washington University's Program on Extremism, who record life sentences (in this sample n=6) as 470 months, as per United States Sentencing Commission practice (Schmitt and Konfrst 2015).

while Internet usage does offer a number of operational benefits, it may also alert unwanted attention.

	Event Success			
Online Behaviour	X^2	*P*	%	**Odds Ratio**
Online Network	15.38	.000	64.2	.256
Online Learn/Plan	6.70	.010	81.5	.134
Reinforce Beliefs	12.01	.001	42	.362
Disseminate Propaganda	8.39	.003	27.2	.412
Share Ideology	8.61	.003	43.2	.425
Seek Legitimisation	8.68	.005	14.8	.412
Social Media	7.97	.004	71.6	.360
Access Ideological Content	6.74	.012	60.5	.445
Prepare Event	15.64	.000	59.3	.274
Overcome Hurdle	5.34	.015	18.5	.455

Table 11 - Event Success and Online Behaviours Significant Correlates

This was expanded upon by considering three other variables that can be considered proxies for success: whether the individual was known to the security services and whether they were eventually arrested for their activity. In all of these tests, some type of online activity has multiple correlates which suggest that acting online may be an impediment to success (Tables 12 and 13).

	Known to Security Services			
	X^2	p	%	Odds Ratio
Online Network	9.25	.002	85.2	2.83
Reinforce Beliefs	8.17	.003	69.3	2.31
Disseminate Propaganda	17.26	.000	50.8	3.78
Seek Legitimisation	6.17	.010	32	2.39
Social Media	8.85	.003	87.7	2.93
Online Learn/Plan	7.31	.007	93.4	3.34
Access Ideological Content	7.81	.004	77.9	2.40
Prepare Event	6.22	.010	80.3	2.24
Overcome Hurdles	5.34	.047	32	1.85

Table 12 - Known to Security Services and Online Behaviours Significant Correlates

	Arrested			
	X^2	p	%	Odds Ratio
Disseminate Propaganda	3.42	.045	42.7	1.99
Support Others	5.16	.017	43.9	2.35
Prepare Event	8.80	.004	79	2.85
Overcome Hurdles	5.34	.014	31.2	2.87

Table 13 - Actor Arrested and Online Behaviours Significant Correlates

When considering why this is the case, qualitative analyses offer a valuable insight. Simply put, several actors within this sample are not security-conscious. Take the case of

Heather Coffman, who was sentenced to four and a half years in prison for facilitation of her unnamed accomplice's travel to Syria. Coffman had several different social media accounts, including Facebook, outwardly expressing support for the group, including an image of armed men with the text "VIRTUES OF THE MUJIHADEEN" and IS's black standard flag. This vocal support caused the FBI to insert an undercover agent in July 2014, whose travel Coffman would attempt to facilitate too.[63] Coffman's case is no outlier – in many cases actors are identified by the FBI because they are outwardly expressing their views on open (or semi-open) social media platforms. In Jensen, James, et al's (2018) study, they find that although the social media usage of US-based extremists is increasing, those that were more active were less likely to be successful in their event. They note that:

> These findings support the conclusion that while social media is a powerful way for extremists to share ideas and communicate, the use of open platforms may leave individuals vulnerable to identification and interdiction by law enforcement. (Jensen, James et al. 2018, p.8)

The findings of this study seem to support that of Jensen and others in this regard; actors use the Internet in a number of ways that may be helpful to law enforcement in building cases.

The next logical question is, in that case, whether being more security conscious can mitigate the ill-effects of acting online. The variable that pertains mostly to security is whether the actor used end-to-end encryption. However, there are no significant correlates between any of these variables, despite this being an online activity. For example, actors that used end-to-end encryption were exactly as likely to be successful as one would expect (X^2 = .033, p = *.871,* OR = .941). One reading of this is that the use of end-to-end encryption may mitigate this effect to some extent. However, it is important not to over-interpret these results; it does not suggest that the use of encrypted software makes events more successful than one would expect from a random distribution, merely that this particular type of online interaction is net-neutral and does not appear to suffer from the same problems as other types of online behaviour.

5.6.3 Multivariate – Predicting Event Success

The bivariate analyses above establish that there is a significant inverse correlation between the two key variables – engaging in an online network and learning/planning online – and the success of the event. Furthermore, there was no significant correlation between a specific online behaviour – the use of end-to-end encryption and event success. To analyse this further, a binary logistic regression is conducted to incorporate these three variables to assess whether one of these behaviours could significantly predict success.

[63] USA v. Heather Coffman, Statement of Facts, Case 3:15-cr-00016-JAG, United States District Court for the Eastern District of Virginia, 2015.

However, given the significant correlation between the three independent variables, it is important to test for multicollinearity. That is to say, if two or more potential predictors of a phenomenon are highly related themselves, then it can produce unstable and biased standard errors (Vatcheva and Lee 2016). The independent variables are tested for collinearity diagnostics against each other, and each iteration returns a variance inflation factor (VIF) of less than 1.386. Although there is no firm consensus of what constitutes an acceptable VIF threshold, Kock and Lynn (2012) note that the commonly recommended maximum values are 10, 5, and 3.3. As such, the independent variables in this study all fall well beneath this threshold and are considered acceptable.

Given that there are more instances of failure than success, the former is chosen as the baseline – therefore a positive Exp(B) ratio is indicative of failure. The first step includes just the two key variables, which can be seen in Table 14, which finds that interacting in an online network is a significant predictor; those that fail are 3.41 times more likely to engage with co-ideologues online. In the second step, the use of end-to-end encryption is introduced (Table 15) and the model still finds that the only significant predictor is interacting in an online network – those that failed were 3.69 times more likely to engage in a virtual network. Although the use of end-to-end encryption makes success more likely than other online behaviours, introducing the variable of end-to-end encryption in this model does not mitigate this effect significantly.

Behaviour	**B(SE)**	**d*f***	**Sig.**	**Exp(B)**
Online Network	1.226 (.416)	1	.003	3.406
Online Learn/Plan	.349 (.550)	1	.526	1.417
Constant	-.712 (.170)	1	.000	.491

Table 14 - Event Success Logistic Regression: Step 1

Behaviour	B(SE)	d*f*	Sig.	Exp(B)
Online Network	1.305 (.427)	1	.002	3.687
Online Learn/Plan	.373 (.551)	1	.499	1.451
End-to-End Encryption	-.318 (.352)	1	.367	.728
Constant	-.498 (.289)	1	.086	.608

Table 15 - Event Success Logistic Regression: Step 2

There are two interpretations for these findings. Firstly, as suggested above, actors are, in many cases, posting carelessly in open or semi-open platforms which make them easily identifiable to security services that are then able to thwart the attempt in some manner. Secondly, for some actors that have been identified as a law enforcement target, they are infiltrated via online communication by an undercover agent (as noted above, there is undercover agent involvement in 61% of cases in which an actor is charged). Take the case of Sean Andrew Duncan, who was communicating with an unnamed co-conspirator on an unspecified encrypted messaging platform. After the conspirator was in custody and co-operated with US interviewers, the FBI planted an undercover agent in conversation with Duncan, pretending to be the conspirator on the messaging platform, eventually leading to Duncan's arrest.[64] These two interpretations are not mutually exclusive; the latter does not explain how the actor becomes identified in the first place. However, it is important to note that the relationship is underdetermined: it is not clear whether the online communication lowers the chance of event success or whether lower chances of event success (i.e. already being on law enforcement radar) determine online communication. It is also worth noting that introducing end-to-end encryption into the model does not affect it significantly, suggesting that, taken alone, it may make the chances of success greater than other online behaviours, but in this model it does not tip the balance towards greater online security.

5.6.4 Event Success versus Online Network sub-variables

Given that interacting in an online network is a predictor of event success, the next logical step is to assess whether one of its sub-variables predicts success too. I follow the lead of Ranganatham, et al. (2017), who note that although it is tempting to include a high number of input variables, this carries a risk of diluting true associations and leading to larger standard errors. As such, I include the variables which displayed a significant correlation with event success in the bivariate analyses: reinforce beliefs; disseminate

[64] USA v. Sean Andrew Duncan, Application for a Search Warrant, Case 1:18-sw-00029-IDD, United States District Court for the Eastern District of Virginia, 2017.

propaganda; and seek legitimisation.[65] Despite each being under the umbrella behaviour of engaging in an online network, which predicts success, and each showing a significant negative relationship with event success in the chi-square tests, there is no single predictor in the regression analysis (Table 16). That is to say, despite engaging in an online network with co-ideologues being highly correlated, no one specific behaviour dominates the others. For example, it is not merely sharing jihadist magazines, but the combination of this, posting on open social media sites, and discussing ideology that causes security services to take note and plan investigations accordingly.

Behaviour	**B(SE)**	**d*f***	**Sig.**	**Exp(B)**
Reinforce Beliefs	.587 (.375)	1	.118	1.799
Disseminate Propaganda	.382 (.375)	1	.308	1.465
Seek Legitimisation	.595 (.415)	1	.151	1.813
Constant	-1.358 (.354)	1	.000	.257

Table 16 - Event Success Logistic Regression 2: Online Network Sub-variables

5.7 Discussion and Conclusion

As discussed in Chapter 3, "online radicalisation" is a nebulous concept with several different interpretations. This chapter has sought to provide clarity and empirical basis for this by analysing the behaviours of 201 IS terrorists to assess how, and in what ways, these actors used the Internet. To begin, it gives a descriptive demographic "snapshot", finding that the sample is relatively heterogeneous and no common profile seems to exist. That being said, there are some recurring themes: it is predominantly male, younger on average and closer to the bottom of the socio-economic ladder. This is, for the most part, in keeping with previous database studies from other times and locations (Horgan et al. 2016; Bakker 2006; Sageman 2004; Gill et al. 2015). The sample is also very much American in terms of country of birth, citizenship, and ancestry. There are also some interesting sizable minorities that are over-represented compared to baseline data, including refugees, converts, and those with criminal records.

RQ1 assessed how this sample of terrorists used the Internet, coding for a range of different antecedent behaviours, including engaging in an online network, learning and planning about their eventual activity, as well as the types of social media platforms that were used. Put simply, the Internet is ubiquitous within this sample: over 90% of actors used the Internet as part of their antecedent or event behaviours. Almost four in five used

[65] The variables of social media use and sharing ideology online were removed because they are too clearly overlapping with the other variables.

the Internet to communicate with co-ideologues, including: using the Internet to reinforce beliefs, disseminating propaganda, supporting others, seeking legitimisation, recruiting others. Similarly, almost nine in ten used the Internet to learn about or plan their eventual activity, including accessing ideological content, taking motivation after witnessing something online, preparing for the event, selecting their target, and overcoming hurdles.

This is congruent with research identified in Chapter 3 which posits that the Internet plays an important facilitative role in pathways towards terrorism (Gill et al. 2017; Gill 2016; Hussain and Saltman 2014; von Behr et al. 2013; Gill and Corner 2015; Gill et al. 2015). More specifically to this dataset of IS actors in the US, it concurs with research which points to social media playing an important role in radicalisation and recruitment (Soufan Group 2015; Vidino and Hughes 2015) as well as the "supply-side" research which highlights IS' active and wide-reaching presence on social media platforms (Berger and Morgan 2015; Carter, Maher, and Neumann 2014; Fisher 2015; Klausen 2015). Moreover, the high levels of preparatory behaviours are congruent with existing research which points to the Internet as a means for instructing individuals to commit acts of terror (Alexander and Clifford 2019; Hughes and Meleagrou-Hitchens 2017; Reed and Ingram 2017).

The wide range of online antecedent behaviours and the diversity of different platforms point to the online radical milieu as a wide ecology. Individuals did not merely use the Internet to access propaganda or discuss ideological matters with peers. Instead, several behaviours were prominent. Moreover, this took place over 28 different identified platforms, from "mainstream" social media sites such as Facebook, Twitter, and YouTube, to end-to-end encrypted platforms like Telegram and WhatsApp, to file storage sites like Google Drive and Dropbox. This mirrors the description of the online ecosystem as described by Fisher, Prucha, and Winterbotham (2019) in which large platforms such as Facebook, Twitter, and Telegram are "beacons", which direct users to material on "content stores", such as archive.org and YouTube. Finally, "aggregators" collect a range of links to different materials around the web and store them on Facebook pages or websites. Given the different affordances that platforms provide, one may question the utility of a sharp online/offline dichotomy (Valentini, Lorusso and Stephan 2020); it may be more worthwhile to consider the wider information environment that an individual engages in, consisting of both online and offline interactions.

Many of the coding variables were chosen to provide a direct comparison to the database research of Gill and colleagues (Gill et al. 2017; Gill 2016; Gill and Corner 2015). This suggests that the use of the Internet is more prevalent within this sample than in studies research a date range further in the past. This is supported by research by Jensen, James, et al. (2018) on US-based extremists, who found a steady increase in social media usage from 2005-2016. The most logical explanation is that the Internet has become ubiquitous for society in general, therefore we should expect terrorists to follow the same trend. However, differences in the richness of data, location, and coding are also possible

explanations that could play a role. Taken together, all of the findings of RQ1 suggest that terrorists use the Internet heavily for a wide range of behaviours on a diversity of platforms and that it is likely that Internet usage has increased compared to previous terrorist populations.

Having established that this sample used the Internet heavily, RQ2 sought to address the claim that 'face-to-face radicalisation has been replaced by online radicalisation' (Sageman 2008b, p.41). To do this, chi-square analyses were used to establish whether individuals that used the Internet were more likely to also engage in the offline domain. The findings reveal that although Internet usage is very high, it does not appear to be a substitute for offline interactions. Rather, if one is exhibiting behaviours in the online domain, they tend to be doing so in the offline one too. This was the case for both network and learning/planning variables, mirroring the findings of Gill and colleagues' (2017) previous research using similar variables.

These findings are congruent with much of the previous research on this topic. Beyond Gill et al. (2017) and Gill and Corner (2015), it also mirrors the qualitative findings of von Behr et al. (2013), who judge that while the Internet increases scope for radicalisation, it is not a substitute for face-to-face meetings. Similarly, Reynolds and Hafez's (2017) study of German foreign fighters tested the hypotheses of "online radicalisation" versus "offline social network", finding the latter to offer greater explanatory power for mobilisation to Iraq or Syria. Other research on foreign fighters – which made up around half of this sample – has also suggested that despite an increase in Internet usage, mobilisation has tended to rely on face-to-face networks (El-Said and Barrett 2017; UN-CTED 2015). Interestingly, the report by the Soufan Group (2015) also makes this assertion but note that the US may be an outlier by relying more on social media. The findings of this research suggest that this may not be the case, and the US is actually in keeping with other countries around the world.

Having established that the online realm does not appear to be replacing the offline domain as the primary venue for radicalisation, RQ3 seeks to explore whether individuals that use the Internet exhibit different experiences to those that do not. In essence, it asks whether the affordances provided by the Internet are more suited to certain types of actors or specific plots. In a small number of cases there is some support that there may be certain differences between the two groups. When breaking down being "a terrorist" into different roles, this research found that both financiers and facilitators – i.e. those that supported eithers by financial and other means – were significantly more likely to engage in an online network. This may suggest that the affordances of the Internet, such as cheap and easy communication, which can be used to offer operational advice (Alexander and Clifford 2019; Hughes and Meleagrou-Hitchens 2017) or facilitate the movement of funds (Keatinge and Keen 2017; Camstoll Group 2016) has made the Internet the first port of call for those aiding terrorist plots. Conversely, attackers were significantly less likely to do so, which may relate to the simplicity of plots in this sample (discussed below).

The starkest results of RQ3 are the null findings of learning and planning behaviours. Previous research has found that lone actors are likely to use the Internet (Gill et al. 2019), doing so more than their group-based counterparts to supplement their lack of co-offenders, from whom they can pool expertise and resources (Gill et al. 2017). This finding did not hold in this sample; those that executed plots alone were just as likely to use the Internet as members of a cell. This is relatively surprising result, potentially due to several "spur of the moment" attacks, like that of Edward Archer,[66] Mahad Abdiaziz Abdiraham,[67] and Esteban Santiago,[68] who displayed little online *or* offline learning and conducted simple plots due to the easy access of weapons. This RQ does find that solo actors – those that conduct a plot alone but with wider command control links were more likely to learn online, potentially because these links involved preparatory learning online. Bivariate analyses also found that there was no relationship between either age or gender and acting online, suggesting that claims that younger people (Gill and Corner 2015; Prensky 2001) or females (Huey and Witmer 2016; Pearson 2016; Bermingham et al. 2009) may have more reason to use the Internet do not seem to hold in this sample.

Importantly, of the 55 attackers in the sample, more sophisticated or riskier plots do not seem to have relied more on the Internet for learning or planning. There are no significant correlates for this variable and any of the following: attack type (armed, unarmed, IED, vehicle based) or attack target (civilian, government, police, army). This is at odds with existing research which posits that more sophisticated plots, like those that require bomb-making skills, or those that plan to hit "hard" targets, are more likely to utilise online learning (Gill et al. 2017). This is particularly stark given the well-documented easy access to instructional material for more sophisticated plots (Conway, Parker, & Looney, 2017; Reed and Ingram 2017). Given that this result is a null finding – i.e. sophisticated attacks were just as likely to learn online as non-sophisticated ones – perhaps the most likely explanation is that the use of the Internet is so high for the sample as a whole that is was used for almost every actor for online learning, regardless of sophistication.

Taking the findings of RQ2 and RQ3 together lends weight to the claim that drawing an easy distinction between online and offline "radicalisation" may not be possible. Not only do actors operate in both domains, but experiences are, in large part, similar for Internet and non-Internet users. Gill and others put this best:

> There is no easy offline versus online radicalisation dichotomy to be drawn. It is a false dichotomy. Plotters regularly engage in activities in both domains. Often

[66] Associated Press, 'I am an American': Man who was 'ready for jihad' before attempting to join ISIL sobs as he's given 15 years in prison, *National Post*, July 28, 2015. Available at: http://nationalpost.com/news/world/i-am-an-american-man-who-was-ready-for-jihad-before-attempting-to-join-isil-sobs-as-hes-given-15-years-prison

[67] USA v. Mahad Abdiaziz Abdiraham. Criminal Complaint, 4th Judicial District Court, Case: 27-CR-17-28647. State of Minnesota, County of Hennepin, 2017.

[68] Ray Sanchez, What we know about the fort lauderdale airport shooting suspect. *CNN,* January 8, 2017. Available at: https://edition.cnn.com/2017/01/06/us/fort-lauderdale-airport-shooting-suspect/index.html.

> their behaviours are compartmentalised across these two domains…Threat management procedures would do well to understand the individuals' breadth of interactions rather than relying upon a dichotomous understanding of offline versus online, which represent two extremes of a spectrum. (Gill et al. 2015, p.35)

This argument is also made by Baugut and Neumann (2019) in their study of jihadist consumption of propaganda, noting that this activity cannot be easily demarcated into either domain; the two are inseparably intertwined and feed into each other. Despite the wide range of affordances that are utilised by terrorists on the Internet, there is little sense to be made by demarcating online radicalisation from offline, but rather, the information environment available to actors contains a wide range of different online platforms and offline interactions which can be utilised.

The question of the role of the Internet was turned on its head for the final research question; while previous research has often focused on the potential danger of terrorists radicalising on the Internet, RQ4 sought to establish whether acting online may be an impediment to success. Previous research by Gill and Corner (2015) and Jensen, James et al. (2018) found that those that use the Internet are less likely to be successful in completing their plot. This was also supported within this dataset; individuals that used the Internet were significantly less likely to be successful. Conducting a binary logistic regression shows that engaging in an online network is a predictor of plot failure. Moreover, several online behaviours were also related to the actor being known to the security services prior to the execution of their plot, as well as the FBI inserting an undercover officer into the plot.

These results suggest that terrorists may be recklessly telegraphing their intentions on the Internet, which in turn, alerts the security services to them to begin an investigation. This point is made by Neumann (2013a) and Benson (2014) who both argue that access to terrorist online materials is a vital part of strategic and tactical intelligence, as well as collecting evidence for criminal trials. However, in recent years, social media platforms have become more adept at proactively removing terrorist – and particularly IS – accounts and content (Conway et al. 2018; Grinnell, Macdonald, and Mair 2017; Berger and Perez 2016). On this reading, security services may be being hampered by content removal because they are not able to collect information that can be easily accessed. Other research suggests that terrorists have migrated to end-to-end encrypted platforms (although these results downplay this to some extent), that are less accessible for security services and do not respond to takedown requests or subpoenas (Clifford and Powell 2019; Europol 2018; Bloom et al. 2017). In essence, removing terrorists from mainstream platforms could be inadvertently forcing them to be more security-conscious.

The overarching theme of this chapter is that the relationship of the Internet to terrorism is multifaceted. One might be tempted to look at the descriptive data and conclude that actors are "radicalising" online as the vast majority are using the Internet both to communicate with co-ideologues and to learn/plan their activity. However, bivariate and

multivariate analyses suggest that this is not so. The online domain has not replaced the importance of offline interactions, as has been suggested previously. Moreover, for the most part, terrorists seem to consistently use the Internet, regardless of the sophistication of their plot, or demographic factors such as age or gender, pointing to a similar experience for those that act and do not. It may even be the case that Internet usage may act as an impediment by alerting unwanted attention from security services. In other words, the truly dangerous terrorists may be the ones that do not use the Internet. However, quantitative analyses can only explain so much – it is also important to assess the evidence qualitatively to both explain the themes that have emerged from this chapter, as well as identifying other themes that may not have appeared in a pre-existing, predominantly binary codebook.

Chapter 6: The Online Dynamics of Terrorist Pathways

6.1 Introduction

The previous chapter conducted a quantitative analysis using a (mostly) deductive codebook that was created to answer research questions devised from the academic literature. This chapter seeks to turn this approach on its head by using an inductive methodology to determine emergent themes from the data to generate theoretical propositions to better understand the role of the Internet in contemporary radicalisation.

6.1.2 Grounded Theory

To do this, I will draw from a methodology inspired by Grounded Theory (GTM), which seeks to approach data with an open mind rather than testing the hypotheses of previous scholars.) GTM is an inductive method of inquiry, dating back to Glaser and Strauss' *The Discovery of Grounded Theory: Strategies for Qualitative Research* (1967). At the time of its creation, Glaser and Strauss believed that there was a trend in sociology that the "Great Men" such as Weber, Durkheim, and Marx, had generated enough theories within their work for new scholars to test, problematise and emulate (Glaser and Strauss 1967). They rejected this, believing that there was much more theory that could be generated from data.

I believe that GTM is an appropriate tool for this thesis for two reasons: Firstly, as Lehane (2017) argues, the methodology is particularly useful in areas of limited scholarship; her research was focused on the CVE industry, which she describes as having experienced a significant growth of academic output but with policy based on unfounded assumptions. As demonstrated in Chapter 3, the same can be said of online radicalisation, which is largely under-theorised and relies on untested dynamics which inform policy. Secondly, an inductive and qualitative approach acts as a useful balance to the previous chapter, allowing for exploration into concepts such as gender or the construction of identities that cannot be easily demarcated into 1s and 0s. Two the approaches do not exist independently, however, but inform each other. For example, Chapter 5 finds that terrorists that use the Internet are less likely to be successful than those that do not. Chapter 6 offers a potential explanation for this: the construction of a radical online identity is part of an ongoing socialisation process, which may be more important than security concerns.

GTM has seen a significant growth since its "discovery" by Glaser and Strauss in the late 1960s, in the decade the proceeded it, there was a 70-fold increase in published papers with "Grounded Theory" as a keyword and by the 1990s, it can become a common feature of qualitative analytic methods (Urquhart, Lehmann and Myers 2010). However, the methodology is not a monolith; there are several differences in interpretations. Ralph, Birks, and Chapman (2015) outline how it has changed in the past half-century:

> From the postpositivism of Glaser and Strauss (Glaser & Strauss, 1967), to the symbolic interactionism and pragmatism of Strauss and Corbin (1990), to the constructivism of Charmaz (2000), the field of GT is interesting in the sense that grounded theorists offer markedly new ontological and epistemological perspectives at specific moments in time that have developed ‘‘followings.’ (Ralph, Birks and Chapman 2015; p.1)

The most famous difference in methods is exemplified by the split between Glaser and Strauss in the 1990s, in which the former objected to the latter's use of a coding paradigm and "conditional matrix" which, according to Glaser, forces data down a singular path (Urquhart 2013). In essence, Glaser wanted the process to remain as unencumbered by rules or guidelines as possible, while Strauss and Corbin (1990) wanted to help their students by creating a 'how to' manual (Urquhart, Lehmann and Myers 2010). Similarly, both Glaser and Strauss were criticised for their phenomenalist approach which assumes that theory is merely waiting to be discovered from data which according to Bryant (2002), does not sufficiently account for the subjectivism in coding. This research follows the Glaserian strand as it is the most flexible and reliant on induction (Urquhart 2013), which seems appropriate given the relatively rigid nature of the quantitative element, which is, in part, a replication of previous research.

It should be noted that this chapter cannot be considered "pure" GTM for two reasons related to its mixed method approach. Firstly, traditionally in GTM, the researcher draws from an uncapped dataset which requires an overlap between data collection and analysis; researchers discover new emerging concepts and decide which kind of data to collect next – a process known as "theoretical sampling" (Urquhart 2013). As demonstrated in Chapter 4, this thesis sets out requirements for data collection that are more rigid in nature. However, I use a process similar to this by utilising the theoretical points to further explore related phenomena. For example, my original investigation into the collection of terrorist propaganda led to the finding that actors would "perform" the propaganda as part of an ongoing socialisation process. This led me to sample the low-level content which actors collected, created, and shared to assess whether the same process could be observed. In essence, after the GTM analysis took me to one theoretical proposition, I then took this knowledge and went back to the well of data to expand upon it.

Secondly, in an attempt to rid itself of pre-existing theories of the phenomenon under study, Glaser and Strauss suggest that existing literature should be ignored as far as possible, suggesting:

> An effective strategy is, at first, literally to ignore the literature of theory and fact on the area under study, in order to assure that the emergence of categories will not be contaminated by concepts more suited to different areas. Similarities and convergences with the literature can be established after the analytic core of categories has emerged (Glaser and Strauss 1967, p.37).

While it is a commendable strategy to let the data speak for themselves, it does ignore many of the realities of conducting doctoral research – such as having enough knowledge of the field to participate in a competitive application process and the fact that many need to conduct a literature review prior to deciding the specific methodologies that are most effective. While most GTM scholars do agree that researchers ought to keep an open mind, taking this to its extreme has been criticised, including by Dey, who suggests researchers 'keep an open mind, not an empty head. Even ideas drawn from the immediate field can provide a useful guide to analysis, providing that we keep an open mind about their cogency and relevance to the data' (Dey 2011, p.9). Adopting the approach that Glaser and Strauss advise would be impossible in a mixed method approach, such as this, in which the quantitative element is driven by existing research and theory.

Given these two factors, it is more accurate to call this thesis GTM-inspired. The methodology draws from the coding process, memoing, constant comparison, and theoretical development that is typically used with this methodology (Lehane 2017), which are outlined in more detail below.

6.1.3 Coding

GTM takes place over various stages of coding. Lehane (2017) notes that 'coding has two purposes: to capture the substantive content of the area under study; and to articulate relationships that can be observed in the data (Lehane 2017, p.70). In other words, understanding the data and how they relate to each other. Urquhart (2013) suggests that following Glaser's 1978 model of having three rounds of coding is the simplest, most effective way to code using GTM. Firstly, *open coding*, which involves the researcher going through data line by line with an open-mind, looking for any emerging themes that appear. This can be as simple as basic, unconnected observations, trying to ascertain what is happening in the data (Lehane 2017). Secondly, grouping the open codes into larger categories – known as *selective coding* or *substantive coding*, which are the basis for comparison to create larger theory (Urquhart 2013). The final stage is *theoretical coding*, in which the categories are considered in relationship to each other for the purposes of theory-building. As Lehane (2017) puts it, 'theoretical coding involves identifying and conceptualising the relationships between substantive codes' (Lehane 2017, p.85).

Another central aspect of GTM is the constant comparison of data. Glaser and Strauss offer this key rule for coding: 'while coding an incident for a category, compare it with the previous incidents in the same and different groups coded in the same category' (Glaser and Strauss 1967, p.106). While this appears simple, they argue that it is vital for identifying the theoretical properties of the data and the relationship of categories to both themselves and others. Dey argues that a virtue of constant comparison is that it protects against over interpretation of data by finding connections that do not exist (Dey 2011). Accordingly, at each stage of GTM coding in this research, data are compared to other data in the same category. The bringing together of the constant comparison and the coding is aided by the process of memoing. Lehane (2017) describes this as an essential feature of GTM and a valuable way of engaging with the data. Rather than simply acting as notes to

remember thoughts, they are used to organise theoretical categories by comparing core concepts against each other, or as Charmaz (2006) notes, the researcher reflects on what they have seen, heard, sensed, and coded to help to formulate their ideas.

6.1.4 Theory Building

As noted above, Glaser and Strauss (1967) saw GTM as a way to move past the "great men" in sociology and suggested that there was considerably more theory that could be generated from inductive enquiry with data. "Theory" is a relatively broad word from the abstract grand theories such as Marxism or poststructuralism which act as a lens to understand the entirety of social reality, to "middle range" theories which aim to understand limited aspects of social life (Bryman 2015). Within these middle range theories, two subtypes can be identified, "formal" theory which is a conceptual, area of sociological inquiry, such as stigma, deviance, or social mobility or "substantive" theory which is developed for a substantive or empirical area of enquiry like patient care, delinquency, or race-relations (Glaser and Strauss 1967). Within substantive theory, the comparison takes place within the one single area under study rather than at a higher, more abstract level. Although formal grounded theory does exist, and is advocated by Glaser (2007), it is the generation of substantive theory which is typically associated with GTM and will be the purpose of this research. It is generally written to be transferrable rather than generalisable. In other words, this research will create working theories from a specific temporal and spatial population which could be transferred to situations with similar contexts, rather than generating theory which speaks to online radicalisation in all contexts.

At first glance, GTM seems to be under-utilised within terrorism studies. Relevant to this research is Koehler's (2014) GTM approach to interviews with former neo-Nazis to identify common themes and patterns regarding the role of the Internet as part of their trajectories, generating several testable theories for future research. De Bie and De Poot (2016) use the methodology to draw from police files, interviews, and trial observations to better understand jihadist networks in the Netherlands in the 2000s. In a study focused on radicalisation, Bartlett and Miller (2012) create a database of terrorist actors and conducted interviews with non-violent "radicals", and a control group, and use GTM to establish how the first group differ from the second and third. Similarly, Windisch et al. (2018) use GTM to analyse interviews with 89 white supremacists in the US to better understand their micro-situational dynamics. On the "supply side" of online radicalisation research, GTM has been used to analyse extremist media content (Macdonald and Lorenzo-Dus 2019; Droogan and Peattie 2016).

Despite the relative scarcity with which GTM appears to be used within this academic field, given further examination, key aspects of the approach are regularly used. For example, one of the most important pieces of research for this thesis, conducted by Meleagrou-Hitchens et al. (2018) consists of data-collection and analysis which categorises travellers to Iraq or Syria into three typologies: Pioneers, Loners, and Networked Travellers. Vidino and Hughes (2015) also do this to some extent, identifying

explanatory categories such as “The Role of Social Media”, “Grooming”, “Travel Agents”, and “Devil on the Shoulder.” Finally, in their database study of jihadist attacks in the West, Vidino et al. (2017) collect and analyse data, before forming a “Tripartite Categorisation of Attacks”, as well as identifying the role of “Radicalisation Hubs” as emergent from the data. While these studies may be described as not pure GTM, they utilise elements of the approach.

Rather than beginning with a specific research question, GTM starts with a general area of interest (Lehane 2017). In this case, it is the use of the Internet by IS actors in the US. The data were then openly coded to identify different aspects of online activity, for example: engaging in propaganda, using social media, and when the actor began to use the Internet to engage with extremist content. However, just as the quantitative analysis does not rely solely on examining Internet usage – i.e. sampling the dependent variable – neither does the GTM analysis. Several related offline activities are coded as well so the importance and role of the Internet can be established. This chapter yields three sections:

1. The socialising role of radical content,
2. Space and gender in the online domain,
3. Online only trajectories and the buyers’ market of the Internet.

The presentation of GTM is typically different to usual academic scholarship and involves the researcher reflectively discussing how and why they chose to collect data, explaining their thought process (Mruck and Mey 2019). With that in mind, the chapter will be set up into the sections laid out above. Each of these sections will begin with an introduction that maps out my thought-process for how the data were discovered, followed by an analysis section in which the data are presented in concurrence with the academic literature, and finally, a synthesis section in which substantive theory is formulated from the analysis.

6.2 The Socialising Role of Radical Content

6.2.1 Introduction

When analysing the 201 case studies line-by-line, it became clear that actors engaged with a range of different types of radical content. This activity was coded descriptively into several different types of categories: e.g. the author (whether it was an “official” piece of IS propaganda, or that of another group, or even just an individual such as the preacher Anwar al-Awlaki); the format (such as whether it was a video, magazine, audio); the contents (executions; religious speeches; infographics); and the name of the content. These descriptive codes paint an interesting picture of the landscape of terrorist propaganda, not least because engaging with radical content is often cited as an important dynamic in the online radicalisation process (For example: Weimann and Von Knop 2008; Torok 2013; Saifudeen 2014; Neo 2016), although existing studies tend to focus on the analysis of the content itself rather than the audience that engages with it (Conway 2016a).

Having established a range of different descriptive codes, these data were compared against each other to better understand how individuals engaged with jihadist propaganda. Below, I discuss two of the selective codes: Firstly, whether this propaganda had an explicit link to the actors' terrorist event. That is to say, whether individuals were directly motivated to act because of content, for example by using the instructional materials that appear in jihadist magazines or using "kill lists" – which were circulated by IS online – to select targets. Secondly, the ways in which radical content is engaged with as part of an ongoing socialisation process between jihadists – for example, looking at where, and with whom, individuals watched it. In essence, these two codes provide two types of (non-mutually exclusive) dynamics for the role of propaganda. The first suggests that it can play a primary role in motivation and providing skills for individuals to conduct acts of terrorism, while the second portrays it as "mood music" for a wider radicalisation process which is reliant on peer-to-peer contact. When comparing the two, the data in this sample provide more support for the latter – there are relatively few plots that can be linked directly to propaganda, but considerably more for whom it was a tool for socialisation.

To explore this further, I decided to theoretically sample beyond "official" content to also analyse how individuals engaged with and created low-level content. While the previous section was important because it considered the audience of terrorist propaganda, this sampling decision takes the decision one step further and considers individuals as potential "prosumers," who simultaneously collect, engage, disseminate, and create radical content online. One example of this activity is actors' social media posts, such as those that are text, image, or video-based. Individuals also created and sent Internet memes, which undercut IS' typical ultra-conservative and serious religious messages with attempts at humour which draw from Western popular culture. Comparison between the engagement of formal and low-level content offers support for the idea that individuals engage with radical content as part of a wider socialisation process – actors construct a radical online identity which mirrors the type of content that can be identified within propaganda – what Macdonald and Lorenzo Dus (2019) call the avatar of the "Good Muslim."

Taken together, this section derives the substantive theory that the propaganda should be seen as a facilitator of an ongoing socialisation process between actors online. Existing online radicalisation theory has posited a unidirectional relationship in which the audience are passive consumers who experience morality salience or sense of moral outrage. This section, while not refuting these claims, points to the wider information environment in which content is not just consumed, but also discussed, replicated, and created. Importantly, this process takes place in a way that blurs the online/offline distinction with activities that cannot easily be demarcated into one domain or the other.

6.2.2 What Kinds of Radical Content do Terrorists Collect?

After coding each of the 201 terrorists' case files line-by-line, each piece of propaganda was noted by name, author (or speaker), group affiliation, and type (i.e. sermon,

execution video etc.) In total, 197 different pieces of content were identified[69] from a total of 60 actors in the sample. Almost every piece of content was either reported to have been watched online or downloaded from an online source or no mention was made of where the actor obtained it. In a small number of instances, physical CDs of sermons and hard-copies of books were found,[70] but it is clear that this is primarily an online activity, which is intuitive given the amount of content which is audio/visual and the inherent advantages the Internet offers in disseminating this type of material.

The most frequently occurring piece of content is the IS execution video of the Jordanian pilot Muath Safi Yousef al-Kasasbeh titled *Healing the Believers' Chests*, which occurred 17 times (9%). Second was *The Flames of War Pt. 1*, an hour-long propaganda video with high production value that was released at the height of IS' strength in September 2014, which was represented 8 times (4%). No other piece of content was present more than 5 times, but there were a total of 45 different pieces of official IS content. This suggests a wide array of content without any single piece – perhaps with the exception of *Healing* – that can be suitably described as fundamental to being an IS actor in the US. Although it is tempting to dispel *Healing the Believers' Chests* and other execution videos as pure grotesque propaganda, it is much more. Ingram notes that the first eighteen minutes of the 22-minute execution video offers a highly methodical justification for their actions, relying on jurisprudential, moral, ideological, and political reasoning. This, he argues, has the effect of increasing the perception of crisis to the in-group (Sunni Muslims) while othering the various out-groups (Ingram 2015). Winter offers a similar analysis, suggesting that this, and many other, videos are an example of IS exploiting a victimhood narrative which justify the gruesome punishment that follows (Winter 2015b).

It is possible that the reason for there being few standout pieces of propaganda – other than *Healing* – was the sheer volume that the group was producing at the height of its power. Both Lakomy (2017) and Conway (2016b) observe that from around the declaration of the caliphate in 2014 until late 2015, the group was able to both produce and distribute large volumes of high-quality content.[71]

[69] Identification is satisfied if either the content was named specifically, or if it was clearly described within the data – for example, many of the court filings mention that actors watched the video of the immolation of the Jordanian pilot Muath Safi Yousef al-Kasasbeh, referring to the execution video "Healing the Believers' Chests". If the description was ambiguous or could have been referring to multiple pieces of content, they were not included. If the content was part of a series, but unnamed, such as reference to *Dabiq* magazine, then it was entered with reference to that (i.e. "*Dabiq* Unnamed").

[70] USA v. Abdul Malik Abdul Kareem, Exhibit List, Case 2:15-cr-00707-SRB, United States Court for the District of Arizona, 2016.

[71] However, in 2016 both the loss of propagandists within the caliphate to targeted drone strikes and the degradation of the group's online presence, this significantly reduced. A number of other studies have suggested that, today, the group's ability to disseminate propaganda has been severely limited (Macdonald et al. 2019; Conway et al. 2018), although this has spurred a number of innovations from sympathisers of the group (Fisher et al. 2019). It will remain to be seen whether future IS terrorists have access to such a wide array of content.

Thirty-eight different authors/speakers of content were identified, with Yemini/American Anwar al-Awlaki the most frequently occurring – 11 times (29%) – followed by IS media spokesman Abu Mohammad al-Adnani and radical Jamaican cleric Abdullah el-Faisal (Trevor William Forrest) the next most frequent with five each (13%) – as can be seen in Figure 17. Awlaki's position as most frequent author is particularly interesting for two reasons. Firstly, he was assassinated by a US drone strike in September 2011, prior to IS' prodigious rise in Iraq and around the time Baghdadi sent a cell to Syria (Whiteside 2016), and secondly, Awlaki was a prominent member of al-Qaeda in the Arabian Peninsula (AQAP) (Meleagrou-Hitchens 2011), around the time of his death and since, AQ and IS have engaged in a number of tensions, including high level spats between the leaderships of each group (Stern and Berger 2015). Awlaki's enduring presence suggests that the top-down ideology of IS may be less important to actors in the US than other factors, such as a charismatic, English-speaking preacher.

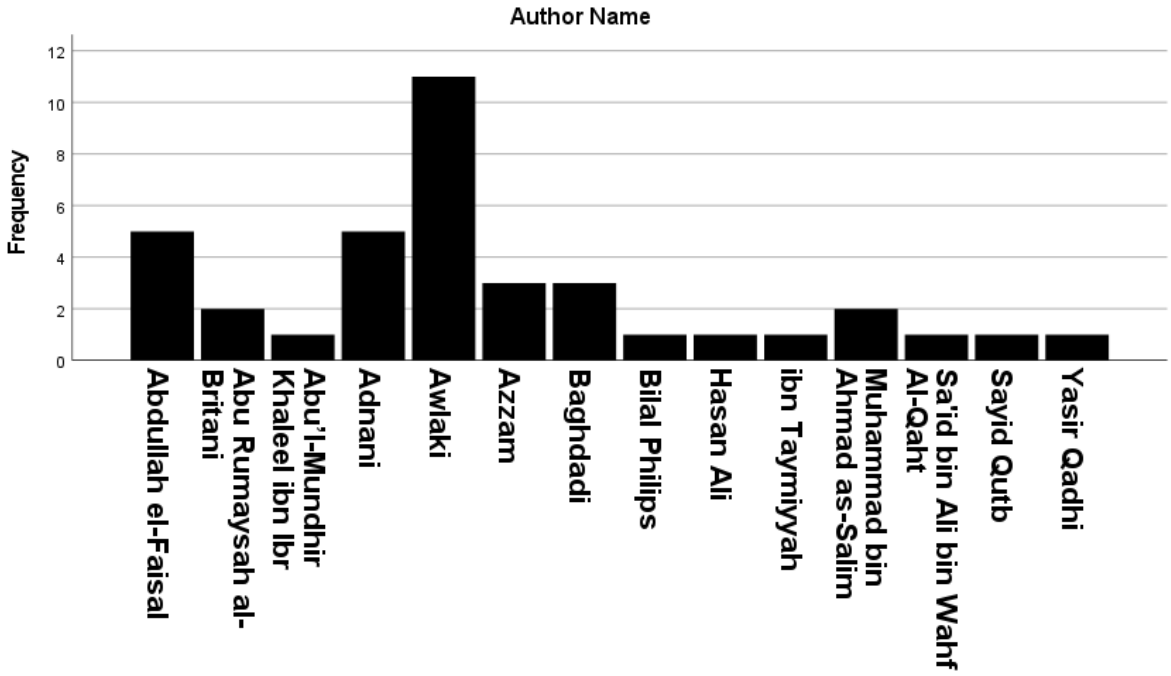


Figure 17 - Author of Radical Content

The presence of Awlaki in contemporary cases of jihadist terrorism in the West – regardless of group – has been noted within the literature. Shane suggests that the aforementioned feud between AQ and IS may have existed on battlefields in the Middle East and North Africa, but did not necessarily carry over to the West (Shane 2016b). In fact, he argues that despite IS' rise to prominence, the group found no English-speaking propagandist of the same appeal, leading to them including an image and his words in the fourth edition of their magazine Dabiq (Shane 2016b). In his study of media content collected from convicted British terrorists, Holbrook also finds Awlaki to be "by far" the most frequently occurring figure with Abdullah el-Faisal in second (Holbrook 2017b), which lends support to the findings of this research, speaking to the importance of charismatic English-speaking preachers for a population that may not have Arabic-

language skills. Gendron (2017) argues that Salafi-jihadist preachers have used the Internet to act as mediators between dense ideological scripture and an audience that needs help digesting it, highlighting Awlaki and Faisal specifically as performing this role.

The presence of Adnani, rather than IS emir Abu Bakr al-Baghdadi, as the most frequently occurring "official" IS member can be explained by the relative lack of attributable pieces of content of the latter. Four of the five instances of Adnani content were the famous speech *Indeed Your Lord is Ever Watchful*, in which he advises actors to stay at home and commit acts of terror in the West rather than travel to Iraq or Syria (Al-Adnani 2018). Baghdadi, on the other hand, rarely made speeches in public and usually relied on audio recorded messages; prior to 2019, his only video appearance was his sermon at Friday prayers at the Grand Mosque in Mosul on July 4th 2014 in which he declared the global caliphate of the Islamic State (Al-Baghdadi 2018). This video was only present once within the sample. Similarly, important texts such as Abdullah Azzam's *In Defence of Muslim Lands* and Sayed Qutb's *Milestones* only appear three times and once respectively. It cannot be overstated how important these pieces of content are to the history of IS and the global jihadist movement, and the fact that these influential actors are dwarfed by Awlaki lends weight to the above claims by Shane that IS were unable to find a propagandist for English-speakers that holds the same appeal.

When looking at the group responsible for creating and disseminating the content, the findings offer a similar account to that of the speakers. While 103 pieces of content (65%) were attributable to IS (mostly execution videos, speeches, or e-magazines), 54 were produced by AQ (34%) – shown in Figure 18. It is worth noting that Awlaki's 11 sermons and written works were not coded as belonging to AQ, but solo enterprises. At first glance, this too, suggests a cross-pollination of content which transcends the tensions between the two groups. However, the 54 pieces of content were all copies of *Inspire e*-magazine, more than the 49 total IS magazines – displayed in Figure 19.[72] Actors in the sample seem to be drawn to two specific types of AQ content: Awlaki and *Inspire*, the latter being in part written by the former. There is little evidence of them listening to speeches by AQ emir Ayman al-Zawahiri or older content from Osama bin Laden. This suggests that, rather than actors in the sample engaging in any jihadist content they can find, they are particularly drawn to a specific type of content.

[72] 42 issues of Dabiq, 3 issues of Islamic State News, and 4 issues of Islamic State Report. No copies of IS' second magazine "Rumiyah" were found. This can most likely be explained by the fact that the sample is weighted heavily towards 2015 and the first issue of Rumiyah was released in September 2016.

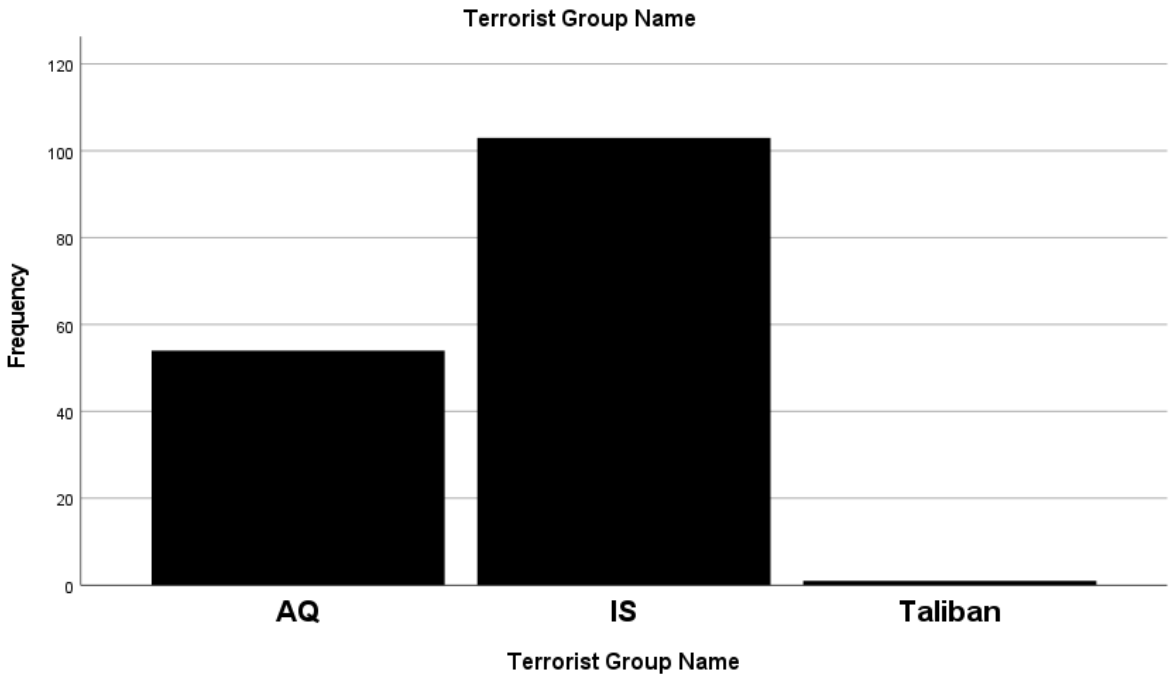


Figure 18 - Radical Content by Terrorist Group

Many scholars have observed that Awlaki's charismatic English-language content – both his sermons and his part in *Inspire* – provided important ideological support to potential recruits. Hughes notes that before actors become violent, there's an amount of "mood music" required, which Awlaki often provides (Hughes, quoted in: Shane 2016). Similarly Meleagrou-Hitchens argues that Awlaki took the global jihadist ideology that had already been created and fostered by bin Laden and al-Zawahiri and simplified it to appeal to the "Facebook generation" of young Western Muslims (Meleagrou-Hitchens 2011). This, too, is present in discussions of *Inspire,* which was clearly written with this generation in mind, employing rap lyrics and superhero narratives (Sivek 2013), with content designed for a less informed and intellectually engaged audience (Lemieux et al. 2014). When compared to IS' magazines – *Dabiq* and *Rumiyah* – which rely heavily on religious scriptures (Ingram 2016a) and frames its articles by way of religious obligation (Macdonald 2016), it is easy to understand why it may appeal to a sample which consists of a large number of novices; at least 29% were converts to Islam and a number of those that were born into Muslim families expressed that they did not have a religious upbringing[73] or that they were ignorant of many of the practices and scriptures of Islam.[74]

[73] For example, see: USA v. Munther Saleh, Defendant's Sentencing Memorandum, Case 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018; USA v. Abdurahman El Bahnasawy, Handwritten Letter, Case 1:16-cr-00376-RMB, United States District Court for the Southern District of New York, 2016.

[74] For example, see: USA v. Islam Natsheh, Defendant's Sentencing Memorandum, Case 3:16-cr-00166, United States District Court for the Northern District of California, 2016; Temple-Raston, D. He Wanted Jihad. He Got Foucault, *New York Magazine,* Nov 27, 2015. Available at: http://nymag.com/intelligencer/2017/11/abdullahi-yusuf-isis-syria.html?gtm=bottom.

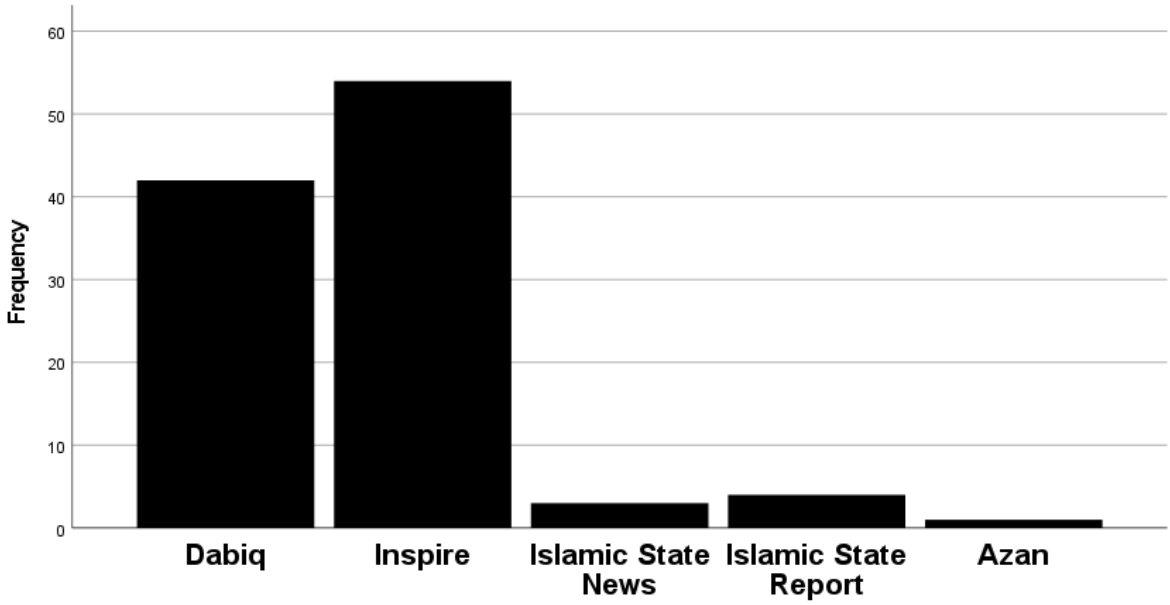


Figure 19 - Magazine Series

6.2.3 Links to Plots

When considering the question of the role propaganda in the radicalisation process, one avenue to explore is whether the content itself has links to plots. This is important because much of academic inquiry into propaganda focuses on the strategic communication of content itself – i.e. why certain speakers or messages *could* be persuasive. However, little has been able to suggest a causal link between consuming radical content and engaging in a terrorist plot. This, again, links back to the "Supply" and "Demand" side of terrorist research online (von Behr et al, 2013) – there is a vast array of research analysing radical content but little data on how it actually influences actors. Therefore, having descriptively coded the different types of propaganda above, this section compares actors' plots to assess whether there are direct connections between propaganda and engaging in acts of terrorism.

One piece of content that there is relatively strong evidence to link to terror plots is *Inspire* e-magazine, which contains instructional material called "open-source jihad"[75] on how individuals can conduct acts of terror within their own countries, foregoing the need for a wider group membership with technological knowhow to execute plots. Noelle Velentzas and Asia Siddiqui, who pleaded guilty to conspiracy to use a weapon of mass destruction, allegedly researched ways to create both a car bomb, as laid out in *Inspire* Issue 12 which they printed out and studied, and a pressure cooker bomb – like the one used in the Boston Marathon Bombing of 2013 – which can be found in *Inspire* Issue 1.[76] However, the two also relied on non-jihadist sources, such as downloading an electronic

[75] In all but four issues (3; 7; 11; and 16)
[76] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint.

copy of *The Anarchist Cookbook,* chemistry textbooks, and YouTube tutorials on soldering.[77] Although the two were able to amass a number of the materials needed for a bomb, the plot was thwarted before it could be constructed.

Similarly unsuccessful was Gregory Lepsky, who pleaded guilty in 2017 to material support for attempting to assemble and detonate a pressure cooker bomb. As with Velentzas and Siddiqui, Lepsky consulted *Inspire* – this time the first issue – for instructions for how to create the bomb, and went as far as purchasing a pressure cooker from an online retailer.[78] Lepsky had downloaded the magazine on his smart phone and backed it up on his computer. As well as consulting *Inspire* for bomb-making instructions, he had also used the Internet to consume other types of radical propaganda, including approximately 3,340 Internet searches on topics such as previous terror attacks, IS' black standard flag, instructions on making anthrax powder, and execution videos.[79]

Other individuals have had more success drawing from *Inspire* magazine's "Open-Source Jihad" section. Ahmad Khan Rahimi, also known as the "Chelsea bomber", was convicted of eight counts including using a weapon of mass destruction and bombing of a public place for setting off pressure cooker bombs in New Jersey and New York. Between 2015 and 2016, Rahimi downloaded every issue of *Inspire*, including the first issue, which includes the aforementioned article on making a pressure cooker bomb titled "How to Make a Bomb in the Kitchen of Your Mom".[80] The court filings note that the article provides detailed instructions on making the types of bombs that Rahimi used for his attacks on 18th September 2016. Like Lepsky, Rahimi also used the Internet to purchase a number of the components of his bombs.[81]

The most well-known plot in this sample that can be directly traced to *Inspire* magazine is the San Bernardino attack, conducted by Rizwan Farook and Tashfeen Malik on 2nd December 2015. Although the attack was an armed assault on the Inland Regional Centre, CA. by the couple, they also constructed at least three pipe bombs that failed to detonate.[82] In the subsequent trial of Farook's friend – Enrique Marquez Jr. – it emerged that Marquez and Farook had used *Inspire's* instructional material to learn how to make an IED using Christmas tree bulbs.[83]

Beyond *Inspire*, other pieces of radical content have been linked to plots, most notably, the IS fatwa against right-wing blogger Pamela Geller. In 2015, Geller organised a competition in which participants drew cartoons of the prophet Muhammad. From

[77] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint.
[78] USA v. Gregory Lepsky, Criminal Complaint, Case 3:18-cr-00114, United States District Court, District of New Jersey, 2017.
[79] USA v. Gregory Lepsky, Criminal Complaint.
[80] USA v. Ahmed Khan Rahimi, Government's Sentencing Memorandum, Case 1:16-cr-00760-RMB, United States District Court, District of New Jersey, 2018.
[81] USA v. Ahmed Khan Rahimi, Criminal Complaint, Case 1:16-cr-00760-RMB, 2016.
[82] Megan Christie et al. Christmas Party May Have Triggered San Bernardino Terror Attack: Police.
[83] USA v. Enrique Marquez Jr., Criminal Complaint, Case: 5:15-mj-498, United States District Court for the Central District of California, 2015.

February of that year, Elton Simpson, Nadir Soofi, and Abdul Kareem plotted an attack on the event, with the online help of British actor Junaid Hussain.[84] Simpson and Soofi opened fire on the competition on the 3rd May 2015, for which IS claimed responsibility. Shortly afterwards, the group uploaded a fatwa[85] to content hosting platform justpaste.it in which they call on supporters to "slaughter" Geller.[86]

In the ensuing days, David Wright, Nicholas Rovinski, and Usaamah Abdullah Rahim plotted to murder Geller – again with online instructional assistance from Hussain – with Rahim purchasing multiple knives from an online retailer.[87] Two days after the call, Rovinski watched a YouTube video of a debate between Geller and convicted UK terrorist Anjem Choudhry, in which the fatwa was discussed, and Rovinski posted in the comments section that Geller was a kufir [unbeliever], implying that she is a legitimate target for violence.[88] The attack never reached fruition because Rahim changed his target to Boston Police Officers and was shot and killed, however, the court filings show that the fatwa and the media coverage that followed it played an important role in the three actors' plot.[89]

A similar type of document to the Pamela Geller fatwa are the "kill lists" that were published by IS and their sympathisers, in which the names, addresses, and other identifying material of US federal employees, including members of the military, were posted online – known as "doxing". The most well-known instance of this was in 2015, when Ardit Ferizi, a Kosovo national, hacked online databases to create a list of 1351 individuals working for the US federal government and sent them to British hacker and IS member Junaid Hussain, who published them on Twitter in August of that year under the name of the "Islamic State Hacking Division".[90] Hussain had previously published the names and addresses of 100 members of the US military in March 2015 as well.[91] It could be argued that having one's personal information displayed on the Internet by a group such as IS is an act of terror in itself; it is an act of incitement with intent to coerce a wider population in pursuit of a religious goal. However, Alexander and Clifford (2019) argue that it is still a relative rarity for US terrorists to use such lists to conduct plots; just Haris Qamar[92] and Nelash Mohamed Das[93] took steps to do so, although neither got to advanced

[84] Seamus Hughes and Alexander Meleagrou-Hitchens, The Threat to the United States from the Islamic State's Virtual Entrepreneurs, *CTC Sentinel*, 10(3), 2017, pp.1-9.
[85] Because the content is anonymous, it is impossible to verify how "official" it is. It is possible it was just IS sympathisers, especially since it was not released via Amaq News Agency.
[86] USA v. David Wright and Nicholas Rovinski, Affidavit, Case 1:15-cr-10153-WGY, United States District Court District of Massachusetts, 2015.
[87] USA v. David Wright and Nicholas Rovinski, First Superseding Indictment.
[88] USA v. David Wright and Nicholas Rovinski, Affidavit.
[89] USA v. David Wright and Nicholas Rovinski, Affidavit.
[90] Audrey Alexander and Bennett Clifford, Doxing and Defacements: Examining the Islamic State's Hacking Capabilities, *CTC Sentinel*, April 2019, pp.22-28.
[91] Audrey Alexander and Bennett Clifford, Doxing and Defacements: Examining the Islamic State's Hacking Capabilities.
[92] USA v. Haris Qamar, Government's Sentencing Memorandum, Case 1:16-cr-00227-LMB, United States District Court for the Eastern District of Virginia, 2017.
[93] USA v. Nelash Mohamed Das, Criminal Complaint, Case: 8:16-cr-00502, United States District Court for the District of Maryland, 2016.

stages of their plot and were infiltrated by undercover sources and arrested. Others, such as Safya Roe Yassin,[94] Terrence McNeil,[95] and Maria Castelli,[96] were prosecuted for disseminating kill lists, while for others, lists were found in the possession of actors that chose other targets, like David Wright[97] and Elton Simpson.[98] Given how well-travelled these lists are and the identifying information they contain, one may expect a greater number of actors to have attempted to utilise them as part of plots, but this does not seem to be the case.

Perhaps the most surprising finding is that there are relatively few cases in which a terrorist event can be directly traced back to a specific piece of radical content. It is possible, however, that the bar for establishing such a link is set too high. For example, Abdul Razak Ali Artan's vehicle and knife-based attack on the campus of Ohio State University took place on the 28th November 2016.[99] Less than three weeks before, the third issue of *Rumiyah* magazine urged actors to undertake vehicle-born attacks, giving the attack in Nice on 14th July 2016 as inspiration. The "Just Terror" section of this issue of *Rumiyah* also suggests that having a secondary weapon, such as a gun or knife. While it is possible that Artan drew inspiration from it,[100] it requires a degree of speculation to even link the two together, let alone answer questions of causation.

More broadly, one could look at the case of Akayed Ullah, who was found guilty of bombing the Port Authority Bus Terminal in Manhattan, NY on December 11, 2017. Although the data do not reveal that Ullah used a specific piece of content to plan his attack, the pipe bomb that he created using Christmas tree lights, a nine-volt battery, wire, screws, are all present in the instructions of "How to Build a Bomb in the Kitchen of Your Mom" from the first issue of *Inspire*. The filings mention that he used the Internet to learn how to build IEDs, but does not mention which sites he visited.[101] Similarly, the filings indicate that Ullah began to watch propaganda videos in, at least, the summer of 2014, including one which suggested that if actors were unable to travel to the caliphate then they should conduct acts of terror in their country of residence, which Ullah did.[102] The court filings do not explicitly lay out that IS content played a role in the event; considering

[94] USA v. Safya Rose Yassin, Criminal Complaint, Case: 16-3024-01-CR-S-RK, United States District Court for the Western District of Missouri, 2016.
[95] USA v. Terrence Joseph McNeil, Affidavit.
[96] USA v. Marie Antoinette Castelli, Plea Agreement, Case: 2:17-cr-00049-DLB, United States District Court for the Eastern District of Kentucky, 2017.
[97] USA v. Nicholas Rovinski, Government's Sentencing Memorandum, Case 1:15-cr-10153-WGY, United States District Court for the District of Massachusetts, 2017.
[98] USA v. Abdul Malik Abdul Kareem, Second Superseding Indictment, Case 2:15-cr-00707-SRB, United States District Court for the District of Arizona, 2015.
[99] Mitch Smith and Adam Goldberg, From Somalia to US: Ohio State Attacker's Path to Violence, *New York Times,* December 1, 2016. Available at: https://www.nytimes.com/2016/12/01/us/from-somalia-to-us-ohio-state-attackers-path-to-violence.html.
[100] Artan died in the attack, which means that no court filings were available, which often provide the most granular and detailed data.
[101] USA v. Akayed Ullah, Criminal Complaint, Case: 1:17-mj-09200-UA, United States District Court for the Southern District of New York, 2017.
[102] USA v. Akayed Ullah, Criminal Complaint

that Ullah was charged with one count of material support to a designated foreign terrorist organisation, they would be incentivised to draw out as much of a connection with specific groups as possible. However, it remains possible that Ullah used the bomb-making instructions laid out in *Inspire* or followed the advice to conduct acts in the US, although this also requires a degree of speculation. It is important to make note of cases like that of Artan and Ullah, while a firm link between the content and their respective plots cannot be drawn, they represent cases in which it is possible and missing data clouds the ability to make a firm judgement.

The notion that jihadist radical content may be a motivating factor for actors to engage in acts of terrorism is posited in the wider literature. In discussing *Inspire*, Lemieux et al. (2014) argue that the magazine offers an Information, Motivation, Skills framework which can influence action. That is to say, it informs the audience with "facts" such as the West's war on Islam; it motivates actors by informing the reader of their obligations; and gives them the skills to act within the "open-source jihad" section. Similarly, Holt et al. (2015) observe that jihadist videos offer three important functions – a diagnosis which identifies the specific grievance as well as a perpetrator who is at fault; a prognosis which states what needs to be done; and finally a motivational call to encourage the reader to act. This holds similarities with the framework laid out by Ingram (2016b), who notes jihadist propaganda perpetuates the violent extremist "system of meaning" which identifies a crisis which is caused by the out-group, and the solution which can only be provided by the in-group, which can cause the reader to be motivated to act. It seems plausible, given the data presented above, that jihadist content can play an important role in motivating terrorists to act. On these readings, this kind of instructional material acts an important part of radicalisation as it builds on the persuasive elements and gives would-be terrorists the ability to act.

It is also important not to overstate the importance of radical content; there are still relatively few instances which can be directly traced back to plots as a driving factor of the eventual activity. An important, and unanswered, question is whether radical content motivates actors that would not have otherwise committed acts of terrorism, or whether they merely provide a replaceable outlet. For example, if *Inspire* was not available for bomb-making instructions, would actors merely download the easily obtainable *The Anarchist Cookbook*? A definitive answer to this question is not only beyond the data that are available in this research, but it is also unknowable. At first glance, it may be tempting to observe that a large number of actors collected and consumed radical content and assume that it plays an important role in plots. However, the relative lack of cases linking content to events suggests that often, they do not motivate, or at least, only play a part in motivating actors. It seems plausible, perhaps even probable, that few actors are motivated by radical content that are not already ideologically aligned with the wider movement. Reed and Ingram (2017), for example, argue that the instructional material that can be found in *Inspire* and *Rumiyah* is of little value unless the respective groups can convince actors to adopt the "system of meaning". Similarly, Lemieux et al. (2014) warn

against exaggerating the importance of magazines like *Inspire*, and suggest that more attention needs to be paid to the wider milieu in which they operate.

6.2.4 Socialisation

Rather than framing propaganda use as being directly linked to plots, it may be more fruitful to consider it through the lens of a socialisation process of the wider movement which transcends the online and offline domains. That is to say, rather than a "hypodermic needle" effect in which viewing propaganda causes people to become terrorists (Aly 2017), it is instead the "mood music" by which individuals ingratiate themselves into the radical milieu.

An example of this is the ways in which individuals discussed radical content with each other. Speaking to an unnamed co-ideologue on social media about the most popular piece of propaganda in this sample – *Healing the Believers' Chests* – Arafat Nagi said that the actions were permissible and that 'do to them as they do to you…they drop bombs and burn people.'[103] Similarly, Terrance McNeil posted stills from the video on Facebook and wrote: 'This is what happens when you bomb women and children and get caught. Alhumdullilah I was worried for a while they might let that murderer go.'[104] These justifications are very similar to those given in the seventh issue of *Dabiq*, which covers the incident, stating that it was in retaliation for bombings of Muslims at the hands of Jordan (Ingram 2016b). Many other individuals either shared the video with others online – for example Islam Said Natsheh,[105] David Wright,[106] or Khalil Abu-Rayyan[107] – or expressed explicit support amongst their radical peers, like Alaa Saadeh,[108] Laith Waleed Alebbini,[109] or Samy el Goarany.[110] This activity demonstrates that individuals were not merely watching the video and reading the magazines, but engaging dialectically with each other about the content itself.

Engagement with radical propaganda often protrudes the online and offline domains. A clear example of this is when individuals held "viewing parties" where co-ideologues would visit their houses to watch videos. This is detailed most explicitly in the case of the group of travellers from the Minneapolis/St. Paul region: 'the men would spend hours

---

[103] USA v. Arafat M. Nagi, Criminal Complaint, Case 1:15-cr-00148, United States District Court for the Western District of New York, 2015.
[104] USA v. Terrence Joseph McNeil, Affidavit, Case: 5:15-mj-01176-KBB, United States District Court for the Northern District of Ohio, 2015.
[105] USA v. Islam Said Natsheh, Government's Sentencing Memorandum, Case: 3:16-cr-00166-RS, United States District Court for the Northern District of California, 2016.
[106] Hughes, Meleagrou-Hichens, and Clifford, A New American Leader Rises in ISIS, *The Atlantic*, Jan 13 2018.
[107] USA v. Khalil Abu Rayyan, Criminal Complaint, Case: 2:16-mj-30039-DUTY, United States District Court for the Eastern District of Michigan, 2016.
[108] USA v. Alaa Saadeh, Criminal Complaint, [Unknown case #], United States District Court for the District of New Jersey, 2015. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Saadeh%2C%20A.%20Criminal%20Complaint.pdf.
[109] USA v. Laith Waleed Alebbini, Motion to Revoke Detention Order, United States District Court for the Southern District of Ohio, Case: 317-cr-00071-WHR, 2017.
[110] USA v. Ahmed Mohammed el Gammel, Criminal Complaint, Case: 1:15-cr-00588-ER, United States District Court for the Southern District of New Year, 2015.

watching a YouTube channel called Enter the Truth…all slick Islamic State productions, focused on the suffering of Syrian children and the moral corruption the West.'[111] The group would sit in a circle and exchange devices with each other to share their propaganda.[112] Similarly, the Garland, TX. attackers Elton Simpson and Nadir Soofi, along with other co-ideologues including Abdul Malik Abdul Kareem, watched ISIS videos and news coverage of terror attacks together. One individual testified that Kareem looked pleased as he watched execution videos and was excited after the Charlie Hebdo attack.[113] Other small cells watched online propaganda together, including Jaelyn Young and Mohammed Daklalla;[114] Munther Omar Saleh and Fareed Mumuni;[115] Mahmoud Elhassan and Joseph Farrokh;[116] and Sixto Ramiro Garcia and Asher Abid Khan.[117]

As well as watching content together, actors would regularly discuss the content that they had watched with others. Haris Qamar, speaking to a confidential witness that he believed was a co-ideologue, repeatedly discussed propaganda he had watched, including *The Flames of War* and an execution in which someone was run over by a tank, which he described as "beautiful."[118] Discussing the execution video *The Procession of Light*, Casey Spain told a fellow prison inmate that he found it funny that the executioners "finished one off" by putting a fish tank on his head and drowning him.[119] Actors discussed and even replicated nashids – Shivam Patel told a confidential source that he had been watching IS videos and that he had learned one of the songs, which he then sang for the source.[120] According to court documents, Aziz Sayyed also 'sang ISIS chants,' as well as

[111] Brendan Koerner, Can You Turn a Terrorist Back into a Citizen? *Wired*, January 24, 2017. Available at: https://www.wired.com/2017/01/can-you-turn-terrorist-back-into-citizen/.
[112] Dina Temple-Raston, He Wanted Jihad, He Got Foucault, *New York Magazine*, November 26, 2017. Available at: http://nymag.com/daily/intelligencer/2017/11/abdullahi-yusuf-isis-syria.html.
[113] USA v. Abdul Malik Abdul Kareem, Government's Sentencing Memorandum, Case 2:15-cr-00707-SRB, United States District Court for the District of Arizona, 2016.
[114] Emma Green, How Two Mississippi College Students Fell in Love and Decided to Join a Terrorist Group, *The Atlantic*, May 1, 2017. Available at: https://www.theatlantic.com/politics/archive/2017/05/mississippi-young-dakhlalla/524751/.
[115] USA v. Munther Omar Saleh and Fareed Mumuni, Government's Sentencing Memorandum, Case: 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018.
[116] USA v. Mahmoud Amin Mohamed Elhassan, Government's Sentencing Memorandum, Case 1:16-cr-0064-AJT, 2017.
[117] Adam Goldman, An American Family Saved their Son from Joining the Islamic State. Now He Might Go to Prison. *Washington Post*, September 6, 2015. Available at: https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2fnational-security%2fan-american-family-saved-their-son-from-joining-the-islamic-state-now-he-might-go-to-prison%2f2015%2f09%2f06%2f2d3d0f48-44ef-11e5-8ab4-c73967a143d3_story.html%3fnoredirect%3don%26utm_term%3d.153ed638a96a)&noredirect=on&utm_term=.153ed638a96a).
[118] USA v. Haris Qamar, Government's Sentencing Memorandum.
[119] USA v. Casey Charles Spain, Position of The United States with Respect to Sentencing and Motion for an Upward Variant Sentence, Case 3:17-cr-00123-JAG, United States District Court for the Eastern District of Virginia, 2017.
[120] USA v. Shivam Patel, Affidavit in Support of an Application for Criminal Complaint and Arrest Warrant, Case 2:17-cr-00120-MSD-DEM, United States District Court for the Eastern District of Virginia, 2017.

discussing violent propaganda videos and stating that there would be no higher honour than to conduct such acts himself.[121]

These sets of cases demonstrate that propaganda can play a role in the ongoing socialisation process between actors. It is an activity between friends; a topic of conversation; or a justification for violence. Most importantly, it is not the one-way transfer of information from the Internet to a user, but rather part of a larger and more complex information environment which includes several types of radical online content which may reinforce each other (such as magazines and execution videos), offline discussions with co-ideologues, and online postings – the latter is discussed in further detail below. When considering the phenomenon of online radicalisation, this demonstrates that there is often a blurred distinction between the two domains that is not easy to rectify because it is not necessarily clear which activities can be seen as "online" and which as "offline."

This is congruous with the findings of Baugut and Neumann (2019), whose interview-based research with 44 German jihadists found that propaganda consumption was often followed by offline discussions about the content with peers and preachers, or vice versa, in which conversations with peers and preachers aroused interest in further radical content. As with actors in this sample, they found that individuals watched radical YouTube videos in groups and discussed them afterwards. Importantly, participants highlighted that the discussions led them to believe they were actively engaging with the content, rather than passive consumers of it (Baugut and Neumann 2019). It is easy to look at the vast array of "slick" and "Hollywood-esque" IS online propaganda and conclude that it has some kind of radicalising agency. However, this perspective is incorrect; even where actors are engaging online, they are also engaging offline, as demonstrated by Chapter 5 and the findings of Gill et al. (2017) and Reynolds and Hafez (2017). In many instances, separating the two domains is impossible: 'These two modes of communication were strongly intertwined across the complete process of radicalization' (Baugut and Neumann 2019, p.16).

The two explanations – that online content can be motivating under some circumstances and that consuming content is part of a socialisation process – are not mutually exclusive. Rather, they are probably inseparable. Clearly, it is important that IS' preference for gruesome execution videos, which are viewed widely in this sample, may lead to one hypothesising some potentially important psychological affect such as mortality salience, which could be linked to support for terrorism (Pyszczynski et al. 2006) – although this goes beyond the scope of secondary research. Similarly, propaganda which aims to sell a utopia narrative (Winter 2015b) or that an apocalyptic war is approaching (Ingram 2016a), which much of the consumed content in this sample does, may resonate with audiences compared to previous groups' propaganda which focuses on other issues, such

[121] USA v. Aziz Ihab Sayyed, Plea Agreement, Case 5:18-cr-00090-AKK-HNJ, United States District Court for the Northern District of Alabama, 2018.

as a war of attrition against the West (Novenario 2016). Even if the content is primarily consumed as social currency, the nature of the content can still be important.

6.2.5 Informal Content

Having sampled and analysed the identifiable "formal" content that terrorists in this sample an interesting perspective appeared – individuals were discussing the propaganda they had watched with their peers. In many instances, actors would take to social media to discuss or justify the content. This led me to consider the individuals in this content as potential content creators, rather than as merely an audience. Conway advocates for this in her call to "deepen" their understanding of online content by considering the position of the audience, she specifically notes that 'a particularly salient question would be whether a majority or minority…are so-called prosumers, that is at the same time both producers and consumers of violent extremist online content' (Conway 2016a, p.10). Therefore, I decided to theoretically sample towards the *informal* content – that is to say, content that is not created by a terrorist organisation but instead by individuals.

The findings from this research suggest that there is much that can be learned from researching the creation and dissemination of low-level content. Actors in the sample used social media to profess their support both for IS and the wider jihadist movement using text-based functions of platforms, by posting images, and by recording and uploading videos. A recurring theme within this activity is the construction of the online self as the "Good Muslim"; actors would post content identifying themselves as jihadists even if it is damaging to actors' self-preservation. Many of these constructed personas also conform to the hyper-masculine gender roles that the group propagates. Another important aspect to low-level content is the circulation of memes and gifs by actors in the cohort, which should be seen as communication acts by both their creators and disseminators. These findings lend support to those presented above on formal content – engagement with informal radical content is part of socialisation within the radical milieu in which they inhabit.

As presented in Chapter 5, the majority (56%) of actors chose to express their ideology on an open or semi-open platform such as Twitter or Facebook. In many instances, this was just the basic text function of platforms. For example, Haris Qamar regularly posted statements supportive of IS and its ideology, including asking Allah to "give strength to the mujahideen to slaughter every single US military officer" and after the group conquered Europe that "Auschwitz will be opened again" for non-believers.[122] Or take Safya Roe Yassin, who using Twitter referenced the Garland attack in May 2015, and noted: "They are only getting bolder because no one was killed at their last event, but if it goes the other way…they have courage now, but if a backpack was left at the scene w/nothing in it, you would have a stampede, lol".[123] Finally, Abdullahi Yusuf, who wrote

[122] USA v. Haris Qamar, Government's Sentencing Memorandum, p.2.
[123] USA v. Safya Rose Yassin, Criminal Complaint, pp.6-7.

in a comment section below an image on Facebook that 'Bashaar asad don't deserve to live.'[124] These three actors, and many more in the sample, used violent emotive language to express their ideology, making little attempt to hide it.

Several actors also used social media platforms to create image-based ideologically-aligned radical content. Many actors took photographs of themselves and their co-ideologues with weaponry and uploaded them to social media platforms. Jalil Aziz purchased materials for a military-style rucksack, including ammunition for an AR-15 rifle, a knife, fingerless gloves, and a balaclava, posting multiple images of them to Twitter.[125] Robert Hester allegedly posted a number of photos of automatic weapons and ammunition to an unnamed social media platform, as well as a photo of a Quran next to a handgun and a knife.[126] Gregory Lepsky uploaded several photos of himself to Facebook dressed in military fatigues with a semi-automatic rifle in one hand and a pistol in the other with the accompanying comment: 'look at these sick photos of me yoo'.[127] None of the actors seemed to be concerned that the content would alert unwanted attention from law enforcement, in fact, a Facebook friend admonished Lepsky that he may have his door "kicked in" by police, to which he responded 'fuk the police they are alostolates[128] and disbelievers'.[129]

Many other actors broadcasted their ideological leanings by using imagery other than, and sometimes combined with, weaponry. One popular photograph was of actors posing with their index finger in the air – known as the tawheed gesture (Wignell, Tan, O 'Halloran et al. 2017), representing the oneness of God, which is central to Salafist ideology (Wiktorowicz 2006). A different photo of Lepsky found on his mobile phone showed him in military dress, with a rifle in one hand and making this gesture with the other.[130] Harlem Suarez also posted photos of himself online making this gesture with a ski-mask to conceal his identity.[131] Actors also posed with IS' flag, their version of the black standard with the Islamic declaration of faith (shahada) written on it (Johansson 2017). When UK border authorities searched Sajmir Alimehmeti's mobile phone and computer, they found photos of him both in front of the flag and one of him making the tahweed gesture.[132] Joseph Jones and Edward Schimenti allegedly took a photo of

[124] USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint, Case: 14-MJ-0124, United States District Court for the District of Minnesota, 2014, p.22.
[125] USA v. Jalil ibn Ameer Aziz, Government's Sentencing Memorandum, Case 1:15-cr-00309-CCC, United States District Court for the Middle District of Pennsylvania, 2017.
[126] USA v. Robert Lorenzo Hester Jr., Criminal Complaint, Case: 4:17-cr-00064, United States District Court for the Western District of Missouri, 2017.
[127] USA v. Gregory Lepsky, Criminal Complaint.
[128] The court filing suggests that Lepsky meant to post "apostates".
[129] USA v. Gregory Lepsky, Criminal Complaint, p.8.
[130] USA v. Gregory Lepsky, Criminal Complaint.
[131] USA v. Harlem Suarez, Government's Sentencing Memorandum, Case 4:15-cr-10009-JEM, United States District Court for the Southern District of Florida, 2017.
[132] USA v. Sajmir Alimehmeti, Criminal Complaint, Case: 1:16-cr-00398, United States District Court for the Southern District of New York, 2016.

themselves in front of the flag with an undercover FBI source to show the source's alleged brother, a purported IS member; the flag was also Schimenti's Google+ profile image.[133]

Actors from the sample also utilised audio-visual technologies to create and upload video content of themselves and others to the Internet. Zakaryia Abdin allegedly visited a gun range in Summerville, SC and videoed himself firing an AK-47 which he uploaded to an unnamed social media platform.[134] Haris Qamar and a confidential FBI source visited several different tourist sites around Washington D.C. and took videos with a view to sending them back to IS for the purposes of official propaganda videos. When taking a video of the Pentagon, Qamar shouted statements in support of IS that could be heard, such as 'bye bye DC, stupid ass kufar, kill 'em all.'[135] Many actors also planned to make videos as part of their plots that never came to fruition. Munir Abdulkader planned to abduct and behead a US military veteran on camera for the purposes of a propaganda video.[136] John T. Booker, who plotted an attack on a US army base, planned to capture a high-ranking military officer before conducting an IS-style execution on him.[137]

6.2.6 Radical Construction

One might be inclined to put these outward expressions of violent ideology down to stupidity. After all, in terms of both self-preservation and winning IS' perceived war against the West, telegraphing such activities online is detrimental as it can alert law enforcement to them.[138] As discussed in the previous chapter, this is precisely what happened to Heather Coffman. It would be more rational to keep as quiet as possible and not draw attention to themselves. However, to claim it is just foolishness is superficial. The common theme of all of these actors – 56% of the sample – that needlessly telegraphed their ideology in an open platform is that they are projecting an idealised version of themselves. Burkell et al. (2014) find that Facebook users tend to create an online persona that is intended for public consumption rather than a "true" representation of themselves. Gündüz (2017) too, argues that people play "characters" on social media which present themselves in ways in which they wish to be perceived. This is true, too, of posting images in which users engage in a reflexive process of portraying certain aspects of selfhood, while ignoring or concealing others – performing acts of "staged authenticity" (Uimonen 2013). On this reading, the performance of "being" a jihadist is important. This can be done by projecting ideologically relevant information

[133] USA v. Joseph Jones and Edward Schimenti, Criminal Complaint, Case 1:17-cr-00236, United States District Court for the Northern District of Illinois, 2017.
[134] USA v. Zakaryia Abdin, Criminal Complaint, Case: 2:17-mj-00081-MCRI, United States District Court for the District of South Carolina, 2017.
[135] USA v. Haris Qamar, Statement of Facts, Case 1:16-cr-00227-LMB, United States District Court for the Eastern District of Virginia, 2016, p.10.
[136] USA v. Munir Abdulkader, Sentencing Proceedings, Case 1:16-CR-019, United States District Court for the Southern District of Ohio, Western Division, 2016.
[137] USA v. John T. Booker Jr. Criminal Complaint, Case 5:15-mj-05039-KGS, United States District Court for the District of Kansas, Topeka Docket, 2015.
[138] For example, Heather Coffman's outward support for IS on Facebook caused a friend to alert the FBI. USA v. Heather Coffman, Criminal Complaint.

on social media, such as violent language towards the "other", posing with weaponry to show strength, or appearing pious by making the tahweed gesture.

Linking together the previous discussion on formal content and this one, the performance of US-based actors may be symbiotically related to what is being projected to them from the official propaganda produced by IS and other groups. Brachman and Levine (2011) argue that the malleable nature of cyberspace allows supporters of jihadist movements to create "avatars" of themselves. These avatars are stylized personas that are crafted to appear as authentically involved in the movement and aim to replicate the behaviours that are considered ideal. In this sense, analysis of jihadist propaganda has been found to visually construct the notion of the "Good Muslim"; a respected non-leader that utilises artefacts such as weaponry and flags that aim to elicit the call for violent jihad (Macdonald and Lorenzo-Dus 2019). Similarly, in his analysis of the IS virtual caliphate, Winter finds that propagandists go to great lengths to portray the strength of their military to perpetuate the aura of supremacy and momentum (Winter 2015b). Within this sample, violence, particularly intertwined with religious and ideological piety, is the "language" with which actors communicate and perform their constructed avatars. The Internet provides an outlet that is fundamentally different to the offline domain; offering a more malleable and an idealised version of how actors wish to be seen by their peers. Interestingly, Brachman and Levine (2011) argue that for some that create avatars, they begin to take steps to reconcile the differences between their online and offline personas. Although none of the plots came to fruition, those that sought to video their terrorist activities can be seen as attempting to do this, granted it is not clear they would have been able to follow through given the opportunity.

As well as the image of the "Good Muslim" being portrayed in formal propaganda, many of the actors constructed this identity in the caliphate and used the Internet to transport it back to their peers in the US. Both Abdi Nur[139] and Mohamed Roble,[140] who travelled from the Minnesota/St Paul area to the caliphate in 2014, posted pictures of themselves on social media platforms posing with rifles and the IS flag, which were seen by their friends back at home and played an important part in their attempted mobilisation.[141] As with the consumption of formal propaganda, this blurs the online/offline distinction; Nur and Roble were using the Internet to portray these identities, but were drawing from deep and longstanding social (and in some cases familial) networks with many years of face-to-face communication. Other individuals portrayed their life in the caliphate too, such as Sixto Ramiro Garcia's Facebook account contained a number of pictures of him,

[139] USA v. Mohamed Abdihamid Farah et al., Criminal Complaint.
[140] USA v. Mohamed Amiin Ali Roble, Criminal Complaint, Case 0:16-mj-00584, United States District Court for the District of Minnesota, 2016.
[141] USA v. Mohamed Abdihamid Farah et al., Criminal Complaint.

including posing with an AK-47[142] and IS flag.[143] Abdifatah Ahmed also posted photos on his Facebook page standing underneath the IS flag with a Quran in one hand and an AK-47 in the other.[144] Not only are these actors representing themselves as the "Good Muslim", but they are also providing a reference point to anyone within their online social network that the goal of living within the caliphate is attainable. These pictures from the caliphate are unlikely to be entirely organic. Klausen (2015) notes that the social media accounts of foreign fighters may give the illusion of authenticity but were more tightly managed than one may realise; only trusted actors were given permission to post. IS understood the importance of informal, organic-looking propaganda as well as formal.

The construction of online personas, like that of the "Good Muslim", also has gendered implications. The role of women and the Internet will be discussed in a later section, but it is important to note that the ways in which actors chose to construct their identities also coalesce with typical gender norms within the jihadist community. Pearson and Winterbotham (2017) find that IS propagates "hyper-masculine" norms, in which they appeal to a sense of brotherhood and promote men to a warrior archetype. It is instructive to look at the projections of men that presented themselves as violent such as Aziz,[145] Hester,[146] and particularly the combination of piety and violence, like Lepsky.[147] As Mahmood argues, this is a gendered act: 'masculinity is highly militarised and linked to violence… men are largely engaged as fighters and protectors of women and children' (Mahmood, 2019, p.12). On this understanding, the projection of actors, both in the US and in the caliphate can be seen as conducting "staged authenticity" (Uimonen 2013) of masculinity as guardians of women and children. Interestingly, this does not mean that female actors necessarily use the Internet to project their typical gender roles, as will be discussed in the section on females and gendered personas below.

6.2.7 Popular Culture

As well as content that actors create and share of themselves on social media, another important aspect of informal online content is the flow of low-level material – referred to as "shitposting" – that travels within IS circles. Unlike the pious representations of the "Good Muslim" from official propaganda, these usually take a somewhat lighter and more jovial tone, often imitating Western popular culture. The most common usage of this is the Internet meme, which is usually an image and text together which attempts to

[142] USA v. Asher Abid Khan, Criminal Complaint, Case: 4:15-cr-00263, United States District Court for the Southern District of Texas, 2015.
[143] Adam Goldman, An American Family Saved Their Son from Joining the Islamic State, Now He Might Go to Prison, *Washington Post*, 6 Sept 2016. Available at: https://www.washingtonpost.com/world/national-security/an-american-family-saved-their-son-from-joining-the-islamic-state-now-he-might-go-to-prison/2015/09/06/2d3d0f48-44ef-11e5-8ab4-c73967a143d3_story.html?noredirect=onandutm_term=.153ed638a96a.
[144] Hughes, S., Meleagrou-Hitchens, A., and Clifford, B., The Travelers, *George Washington University Program on Extremism*, 2018.
[145] USA v. Jalil ibn Ameer Aziz, Government's Sentencing Memorandum.
[146] USA v. Robert Lorenzo Hester Jr, Criminal Complaint.
[147] USA v. Gregory Lepsky, Criminal Complaint.

humorously capture a popular cultural symbol. For example, Nicholas Teausant posted a picture to his Instagram account with the text "keep calm and kill kuffar",[148] appropriating the popular "keep calm and carry on" meme – perhaps the irony not lost on Teausant that the cultural symbol originates as a piece of British Second World War propaganda,[149] in which their army occupied a number of Muslim-majority countries; the notion of the West being at war with Islam is central to most jihadist groups' ideology (Glazzard 2017; Ingram 2016b). Similarly, Safya Yassin posted a meme appropriating the poster to Alfred Hitchcock's North by Northwest[150] but with a photo of President Obama imposed as running away from a drone.[151]

While some memes are clearly an attempt at humour, others are more politically overt, such as Muhanad Badawi posting an altered image of Israeli Prime Minister Benjamin Netanyahu standing next to a dog, with President Obama's face imposed.[152] Daniel Franey, too, regularly posted memes which were critical of the enemies of IS, such as the US, France, Iran, and Russia,[153] while Mohamed Maleeh Masha posted a meme of the outline of the US dollar with the text "Interest and Tyranny".[154] Others forecasted violence, albeit in a lighter and less realist tone than much of the content above, such as Munther Omar Saleh, whose phone contained an image of a headless Statue of Liberty holding the IS flag with New York City burning in the background with the words "Coming Soon" – as if imitating a movie poster.[155] Around Christmas time, Samy El-Goarany posted a picture to his Tumblr of a masked figure with a knife holding up Santa Claus' severed head with the caption "Merry Christmas".[156] Finally, Everitt Aaron Jameson allegedly posted a gif – an animated image format – of an audience giving a standing ovation to someone posting an article regarding the 31st October 2017 attack in New York, NY allegedly conducted by Sayfullo Saipov.[157] Even in the instances where violence is clearly

[148] USA v. Nicholas Teausant, Criminal Complaint, Case 2:14-mj-0064, United States District Court for the Eastern District of California, 2014.
[149] Know Your Meme: Keep Calm and Carry On. Available at: https://knowyourmeme.com/memes/keep-calm-and-carry-on.
[150] Know Your Meme: North by Northwest. Available at: https://knowyourmeme.com/photos/1452448-bertstrips.
[151] USA v. Safya Rose Yassin, Criminal Complaint.
[152] USA v. Nader Salem Elhuzayel and Muhanad Elfatih M.A. Badawi, Transcript of Proceedings, Case 8:15-cr-0060, United States District Court for the Central District of California, 2016.
[153] Adam Ashton, Suspected ISIS Sympathiser from Montesano was Hospitalized for Mental Health Problems, Records Show, *The News Tribune,* 12 Feb 2016. Available at: https://www.thenewstribune.com/news/local/military/article60143536.html.
[154] Robert Snell, FBI Hunts Doctor from Flint Area Tied to Islamic State, *The Detroit News,* 23 June 2016. Available at: https://eu.detroitnews.com/story/news/local/michigan/2016/06/23/fbi-hunts-doctor-flint-area-tied-islamic-state/86270418/.
[155] USA v. Munther Omar Saleh and Fareed Mumuni, Government's Sentencing Memorandum.
[156] Katie Zavadski, His Mom and Dad Hid a Terrible ISIS Secret, *The Daily Beast*, 17 Jan 2017. Available at: https://www.thedailybeast.com/mom-and-dad-hid-a-terrible-isis-secret.
[157] USA v. Everitt Aaron Jameson, Criminal Complaint, Case 1:18-cr-00001, United States District Court for the Eastern District of California, 2017.

supported, it is done in a more light-hearted manner, as if to almost parody the gruesome IS execution videos that were commonplace within these circles at the time.

Although the vast majority of research into radical content focuses on "formal" content, a small number of studies have argued for the importance of understanding low-level peer-to-peer content such as the above. Lakomy (2017a) finds that memes are an important part of IS' visual propaganda, also drawing together the connection with popular culture icons such as films, music, and ideas, suggesting they are directed at unsophisticated, young audiences. Several studies reference a popular IS meme – which does not appear in this sample – that plays on the video game *Call of Duty*, which shows two IS fighters with the text: 'This is our call of Duty, and we respawn in Jannah [Heaven]' (Wignell, Tan and O'Halloran 2017; Lakomy 2017b; Dauber et al. 2019). The two men in the picture are faceless and one of the two is making the tawheed gesture and holding a rifle (Wignell, Tan and O'Halloran 2017), which could be interpreted as representing the "Good Muslim" (Macdonald and Lorenzo-Dus 2019), and while it carries a serious message of a promise of war that is undeterred by the threat of death (Wignell, Tan and O'Halloran 2017), it also plays on the popularity of a popular Western (and worldwide) game, offering an opportunity to recruit from outside a narrow base (Dauber et al. 2019), potentially attracting a generation that grew up with videogames such as *Call of Duty*.

Although memes and other low-level content may serve recruitment functions for groups like IS, this perspective overlooks the agency of the actors that create and repost them. Grundlingh (2018) argues that memes are constructed by their creators as speech acts. Similarly, Nissenbaum and Shifman (2017) note that they can highlight the collective identity of the milieu in which they inhabit and serve significant social functions such as reminding members of their affinity. As with the construction of the "Good Muslim", participation with "shitposting" content should be seen as actors constructing their identity in relation to the social network. In Huey's (2015) study of IS memes, she argues that they are powerful because they offer a transgressive counter-culture appeal, asking their audience to laugh at the dark humour, bonding with their audience while denigrating the butt of the joke, feeding the desire of disaffected youth to be seen as cool and edgy amongst their peers. The literature often does not go into the creators of memes, and it is seemingly assumed that it is done to recruit new members to the movement. However, there is little evidence to suggest they are made by IS; their buoyant and satirical nature is not in keeping with the apocalyptic and religious communications of the group (Ingram 2016a). This is important, as it suggests that groups have little control over this type of content; rather it is the currency of a wider movement, which actors use to socialise with peers.

6.2.8 Synthesis

This section has inductively investigated terrorists' engagement with radical content. It began by descriptively coding each of the identifiable "formal" propaganda and then comparing how actors engaged with it, finding that there were some cases in which the content could be deemed to play an active role, but these were relatively few in number.

The ways in which individuals consumed radical content could better be described as an ongoing socialisation process in which content is consumed, discussed, and shared amongst peers. This led to the decision to theoretically sample informal (i.e. not created by terror groups or renowned speakers) content. An analysis of this shows that many individuals created content to construct a radical persona for their online audience. Moreover, actors also engaged in "shitposting" by creating and sharing memes and gifs, which draw from popular culture in a more light-hearted and jovial manner than the tone of typical IS propaganda.

When considering what these findings present as a theory of online radicalisation, the data suggest that rather than radical content having a direct cause and effect relationship to motivate individuals towards terrorism, as is often explicitly or implicitly assumed as a radicalisation dynamic (For example: Weimann and Von Knop, 2008; Torok, 2013; Saifudeen, 2014; Neo, 2016), the consumption of propaganda should be seen as "mood music" – an important component of socialisation, but not necessarily a direct causative effect. Although this research cannot test the psychological mechanisms at play such as mortality salience (Pyszczynski *et al.* 2006) or creating a sense of moral outrage (2008), it does posit that there are important social dynamics. Regardless of whether propaganda can change attitudes or directly motivated individuals – for which there is little empirical evidence (Rieger, Frischlich and Bente 2013; Frischlich et al. 2015; Reeve, 2019) – it can be conceptualised as "mood music" for individuals to converse and bond with each other, while presenting a cultural artefact for them to construct an idealised persona.

The notion that radicalisation is a social phenomenon has been discussed in the existing literature. Helfstein (2012) creates a model of radicalisation which explicitly highlights the importance of socialisation and states that it cannot easily be separated from ideology. Similarly, McCauley and Moskalenko's (2008) "pyramid" of twelve radicalisation dynamics of radicalisation includes only two personal-level factors and ten group-based ones. Webber and Kruglanski's (2017) "3N" model interlinks the "network" (i.e. social aspect) with psychological "needs" and ideological "narrative." Sageman's (2004) "bunch of guys" theory posits that individual pathways are invariably driven by feelings of kinship and brotherhood with their co-ideologues, while Wikström and Bouhana's (2017) situational action theory seeks to better explain radicalisation via the relationship between individuals and their environments.

Given this theoretical scholarship, it is intuitive that engagement with radical content would also play out in a social manner. Rather than merely absorbing information from online propaganda, individuals met to watch and discussed it with friends, as well as demonstrate that they understood it by replicating key themes via text, video, and audio. Moreover, actors constructed idealised versions of themselves to project to their respective audiences to demonstrate their piety or commitment to the cause. This too, may explain why Awlaki was, by far, the most popular propagandist in the sample; this largely US-based cohort (as demonstrated in Chapter 5) needed easily digestible, English-language content, which could be passed around between actors and discussed online

and watched at offline viewing parties as a social activity. In essence, while previous research has pointed to the importance of radical content as a one-way form of communication, the data presented above demonstrate that each terrorist operates within a holistic and complex information environment.

When considering this information environment, the notion of "online" radicalisation becomes conceptually difficult to defend. While Chapter 5 demonstrated that individual engage in both online and offline antecedent behaviours, a qualitative examination shows that many activities cannot be easily demarcated as "online"; individuals met in offline settings to watch propaganda, or they would meet face-to-face to discuss content they had previously watched and give recommendations. As discussed in Chapter 3, scholars have argued that it makes little sense to consider there as being a distinguishable state of being online and offline in the contemporary world; both domains enmesh to form one single, unified reality (Jurgenson 2012; Rey and Boesel 2014). As Valentini, Lorusso, and Stephan (2020) note, terrorists do not "go online" as a deliberate act, but the two spaces conflate in unprecedented ways to the point of becoming inseparable. This chapter provides further support to this argument.

As per the Onlife thesis, the contemporary information environment – what Floridi (2007) calls an infosphere – has changed dramatically and blurred the distinctions between the two domains. However, these changes may help to explain some of the social behaviours that actors in this sample exhibited when engaging with radical content. Importantly, as Thorseth (2015a) argues, the contemporary information environment has also blurred the distinction between public and private communications. She argues that topics such as sexuality and political affiliations that were previously reserved for private, face-to-face now exist more prominently on public platforms. While, at first glance, it may appear foolish that actors are showcasing their jihadist bona fides on social media because it would be more likely to lead to apprehension. However, on Thorseth's reading, the blurred distinction between public and private means that socialising with peers may take precedence over security concerns on social media.

Grounded Theory

1) *Actors consume, create, and share radical content as part of an ongoing social radicalisation process which often blurs the distinction between online and offline*

6.3 Women and Gendered Online Personas

6.3.1 Introduction

The previous chapter – which quantitatively analysed the online behaviours of actors within this sample – used a binary coding system for several online behaviours as well demographic factors including gender. It found that there were no significant correlates between online antecedent behaviours such as engagement in an online network or learning about or planning their event online with gender – i.e. female and male actors use the Internet at approximately the same rate. However, a binary quantitative coding

system may be ill-equipped to fully explain how gender operates within the online domain. Moreover, the previous section in this chapter, which analysed actors' engagement with radical content, found that individuals used social media to construct radical identities as a means of socialising with their peers. In the context of female jihadists, this is interesting because they are traditionally excluded from offline spaces because of strict gender segregation, therefore it leaves open the possibility that the Internet may offer females a social space in which they are freer to explore their ideological motivations.

Given this, I decided to focus on the female terrorists in the database. When conducting descriptive coding, a range of different data points emerged. These included: online activities such as using social media, including the individuals' reach and influence amongst their peers; offline activities – both as a means of comparison to online and understanding whether they had barriers to entry; how actors interacted with their male counterparts. Each of these cases were then compared to each other, leading to three distinct selective codes based on the ways in which female actors engaged online: "Influencers" – who are important and active members of the radical online milieu and rely heavily on the Internet; "peer-to-peer communicators" who use the Internet, but not as actively as the influencers and do not hold as much sway; and finally, "offliners", who have little-to-no online footprint. The findings show that female terrorist actors should not be treated as a homogenous block and have different motivations which manifest in different online behaviours. Having created these categories and engaged with the academic literature, the analysis then reflects on how the females in the sample align with the online activity "roles" as outlined by Huey and colleagues (2017).

The core category of this section – i.e. 'the prime mover of most of the behaviour seen and talked about in the substantive area' (Lehane 2017, p.80) – is the concept of "space" and how different radicalising women use it. The substantive theory generated from the data shows that for some, the Internet can provide a platform for female actors to construct a less restrictive gender identity than may be possible in offline Salafi jihadist circles. However, women are not a monolith and others seemingly chose to avoid this type of activity. As with the previous section on the role of radical content, it provides a facilitative opportunity which could exacerbate radicalisation for some, but they still had to make an active decision to do so.

6.3.2 Influencers

Seven women within the sample used social media platforms widely and engaged with hundreds or even thousands of other actors, with some becoming important influencers within the online jihadisphere. One example is Keonna Thomas, who operated the Twitter accounts "Fatayat Al Khilafah" and "Young Lioness". Thomas' court filings detail her repeated endorsements of IS; her attempts to raise money for the movement; as well as

extolling the virtues of martyrdom.[158] An example of her output can be seen in this tweet on December 2, 2014:

> If we truly knew the realities ... we all would be rushing to join our brothers in the front lines pray ALLAH accept us as shuhada [martyrs].[159]

Thomas clearly had influence, given that the filings also draw on conversations that she had with a number of important men, including radical preacher Abdullah el-Faisal (Trevor Forrest),[160] virtual entrepreneurs Mujahid Miski (Muhammed Abdullahi Hassan),[161] and Abu Khalid al-Amriki (Shawn Parson), the latter of whom she married online via Skype and intended to join in Raqqa before her arrest.[162] The filings do not state how large her reach was but do suggest that she had a 'large online following'.[163] Given this, and her connection to key figures within the movement, Thomas should be seen as a key influencer. What is more, she seems to have achieved this entirely through the means of the Internet; the filings make no reference to any offline networks or activity and repeatedly iterate her online communications since entering the radical online milieu around 2010.[164]

A similar case is that of Safya Roe Yassin, who posted on several different platforms including Facebook, Telegram, Google+, but was prolific on Twitter. As with Thomas, the court filings lay out Yassin's post history, noting that her Twitter accounts were regularly suspended due to terms of service violations and that the FBI identified 97 different account IDs that she was using to post in support of IS.[165] She also regularly changed her handles throughout the day.[166] Yassin tweeted support for British convicted terrorists Anjem Choudary and Mizanur Rahman when they were charged, as well as posts that were violent in nature, including the post mentioned in the radical content section in which she mocked the "Freedom of Speech Rally Round II" – the "first round" referring to the Garland, TX attack by Elton Simpson and Nadir Soofi – by tweeting:

---

[158] USA v. Keonna Thomas, Criminal Complaint.
[159] USA v. Keonna Thomas, Criminal Complaint, p.3.
[160] Jeremy Roebuck, Facing Sentencing, N. Philly Mom Married to Islamic State Soldier is No Aberration, *The Enquirer*, September 4, 2017. Available at: http://www.philly.com/philly/news/pennsylvania/philadelphia/facing-sentencing-n-philly-mom-married-to-isis-soldier-is-no-aberration-20170905.html.
[161] Hughes and Meleagrou-Hitchens, The Threat to the United States from the Islamic State's Virtual Entrepreneurs.
[162] USA v. Keonna Thomas, Government's Sentencing Memorandum, Case 2:15-cr-00171-MMB, United States Court for the Eastern District of Pennsylvania, 2017.
[163] USA v. Keonna Thomas, Government's Sentencing Memorandum, p.1.
[164] USA v. Keonna Thomas, Defendant's Sentencing Memorandum, Case 2:15-cr-00171-MMB, United States Court for the Eastern District of Pennsylvania, 2017.
[165] USA v. Safya Roe Yassin, Criminal Complaint.
[166] USA v. Safya Roe Yassin, Criminal Complaint.

> They are only getting bolder because no one was killed at their last event, but if it goes the other way…" [and] "they have courage now, but if a backpack was left at the scene w/nothing in it, you would have a stampede, lol"[167]

Yassin was eventually arrested and charged for disseminating an IS "kill list" – in which an actor obtained over 150 names, phone numbers and addresses of US air force personnel in August 2015.[168] Yassin distributed the list by retweeting a link from Justpaste.it by Junaid Hussain.[169] In the following days, she then made a series of posts with the captions "Wanted to Kill" and "hunt him down and kill him" targeting specific federal employees that were mentioned in the list.[170] As with Thomas, the filings do not make mention of how large her reach was, but Alexander notes that while 'it's hard to identify leaders within the [jihadist] Twitter community…she's certainly a prolific voice'.[171] Similarly to Thomas, there is little evidence to suggest that Yassin had any offline connections to the movement and her status is likely due to her online efforts.

Waheba Issa Dais also maintained an active presence across several different social media accounts and played an active role in recruitment. The filings outline that Dais was active on Facebook, where she hacked a number of non-radical users' accounts to circumvent suspensions for terms of service to spread propaganda.[172] She also used Twitter and an unnamed social media platform – presumably Telegram – on which Dais ran a channel named "Shu'a' Al-Khilafah for lone wolves." The channel had 89 members, 4 photos, 10 videos, and 445 files, at least 92 of which 'relate to explosives, guns, attack planning, and target selection.'[173] Dais was also in control or posted links to a number of other social media channels, including those that had *nasheeds* and speeches from IS leaders.[174] The filings lay out that Dias was in contact with a number of actors, discussing both travel to the caliphate as well as methods and techniques for creating bombs for terror attacks.[175] Eventually, when in conversation with an undercover agent who stated that they could no longer live in the land of the infidel, Dais responded by offering operational advice for the undercover agent's would-be attack, including staying secretive, potential targets, and that: 'making bombs is easy, and you can also start with poisons,'[176] linking the undercover agent to Dais' above mentioned channel. As with

---

[167] USA v. Safya Roe Yassin, Criminal Complaint, pp. 6-7.
[168] CNN News, Hacker Allegedly Gave ISIS a 'Kill List' of U.S. Troops, October 16, 2015. Available at: https://edition.cnn.com/videos/us/2015/10/16/isis-hacker-malaysia-dnt-todd-tsr.cnn.
[169] USA v. Safya Roe Yassin, Criminal Complaint.
[170] USA v. Safya Roe Yassin, Superseding Indictment, Case No. 16-3024-01-CR-S-MDH, United States District Court for the Western District of Missouri, 2016.
[171] Audrey Alexander, quoted in: Katie Zavadski, The American Anti-Vaccine Mom Turned ISIS Superstar, *The Daily Beast*, March 29, 2016. Available at: https://www.thedailybeast.com/the-american-anti-vaccine-mom-turned-isis-superstar.
[172] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint, Case 2:18-cr-00143, United States District Court for the Eastern District of Wisconsin, 2018.
[173] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint, p.13.
[174] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint.
[175] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint.
[176] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint, p.12.

Thomas and Yassin, the filings do not reveal how big her network was, but she was again clearly an important part of the milieu; a Facebook friend said that it suited her well to be the press manager of IS,[177] while Hughes notes that Dais had been a key voice online and that 'American women supporters in general, but her in particular, tend to be the glue that hold different online spaces together.'[178]

Heather Coffman also maintained an active presence on social media, although Facebook was her primary platform. The court filings note that Coffman maintained at least 10 different accounts with both male and female pseudonyms which were used 'to establish contacts around the world'.[179] She posted several pictures supportive of IS, its leaders, and the ideology more broadly, including the group's black standard flag with the text: 'Allah has preferred the Mujahideen over those who remain [behind] with a great reward. Degrees [sic] from Him and forgiveness and mercy. And Allah is ever Forgiving and Merciful,'[180] which is clearly meant as an encouragement for actors to travel to the join IS. Coffman was in an online romantic relationship with an unnamed foreign national, and the filings observe that together they planned his travel to the caliphate, including Coffman reaching out to her contacts on Facebook that were already in the caliphate to aid this.[181] Although the filings only show snippets of conversations, they heavily imply that Coffman was driving the situation, particularly as the unnamed man backed out of his travel, which resulted in Coffman complaining to an undercover agent:

> I gave him every opportunity to go there remember? I set him up with the brothers who gave him a contact name and number in Turkey to get him across the border when it was time for training…But I think [he] was just joking about us going.[182]

Coffman then attempted to facilitate the undercover agent's travel to Syria, for which she was charged with material support to a foreign terrorist organisation.[183] The filings paint her as an important influencer too, noting that her social media activities were neither casual nor infrequent, and that 'her online presence was significant'.[184]

Not all influencers were caught in the United States; Hoda Muthana allegedly successfully travelled to Syria after leaving Alabama on the pretence of a college field trip in November 2014. Both prior to and after her travel she was an "active part" of the English speaking Twitter community,[185] which is particularly striking given that Muthana's parents –

---

[177] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint.
[178] Seamus Hughes, quoted in: Liam Stack, Wisconsin Woman Used Hacked Facebook Accounts to Recruit for ISIS, Prosecutors Say, *New York Times*, April 22, 2019. Available at: https://www.nytimes.com/2019/04/22/us/wisconsin-woman-isis.html.
[179] USA v. Heather Coffman, Position of the US on Sentencing, Case: 3:15-cr-00016, United States Court for the Eastern District of Virginia, 2015.
[180] USA v. Heather Coffman, Statement of Facts, p.3.
[181] USA v. Heather Coffman, Statement of Facts.
[182] USA v. Heather Coffman, Statement of Facts, pp.6-7.
[183] USA v. Heather Coffman, Statement of Facts.
[184] USA v. Heather Coffman, Position of the US on Sentencing, p.3.
[185] Meleagrou-Hitchens, Hughes, and Clifford, The Travellers.

whom she lived with – banned her from using social media or to speak to anyone who was not a relative.[186] Prior to leaving, Muthana's account had thousands of followers and interacted with like-minded people around the world,[187] including IS members and supporters, such as Aqsa Mahmood, who left Scotland to join the group in 2013.[188] After her arrival, Muthana remained active, tweeting in support of the Charlie Hebdo attack in January 2015;[189] mourning her husband, who died in a Jordanian air strike 87 days after they married;[190] and uploading a picture of her and three other passports to Twitter with the caption: "Bonfire soon, no need for these anymore".[191]

Other women also kept an active presence on social media, although perhaps slightly below the level of the five actors identified above. One such was Ariel Bradley, a convert to Islam who successfully travelled to Syria in April 2014. Prior to her travel, she used the Internet to forge connections to learn about Islam and find a husband, as well as frequently updating her Tumblr account. However, after her arrival in the caliphate, the content became distinctly more jihadist in nature. Bradley, who was originally from Chattanooga, TN, tweeted the day after the attacks on July 16, 2015:

> Gifted this morning not only with Eid but w/ the news of a brother puttin fear n the heart of *kufar* n the city of my birth. *Alhamdullilah* [thanks be to God].[192]

Furthermore, when she tweeted complaints about the sound of bombs dropping, she responded to prayers for her safety with:

> Not death I should fear but the state I meet it in. May Allah guide us and give us *shaheed* [martyrdom]. Ameen[193]

Similarly, unsuccessful traveller Jaelyn Young also maintained a social media presence prior to her attempted departure in August 2015.[194] Young was married to another actor in the sample, Muhammad Dakhlalla, but it was Young that seemingly drove both actors towards attempting to join IS,[195] and her online presence was an important part of this.

---

[186] Jytte Klausen, A Behavioral Study of the Radicalization Trajectories of American "Homegrown" Al Qaeda-Inspired Terrorist Offenders, 2016.
[187] Vidino and Hughes, ISIS in America.
[188] Ellie Hall, Gone Girl: An Interview with An American in ISIS, *Buzzfeed News*, April 17, 2015. Available at: https://www.buzzfeednews.com/article/ellievhall/gone-girl-an-interview-with-an-american-in-isis.
[189] Alexander, Cruel Intentions.
[190] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[191] Alexander, Cruel Intentions, p.18.
[192] Ellie Hall, How One Young Woman Went From Fundamentalist Christian to ISIS Bride, *Buzzfeed News*, July 20, 2015. Available at: https://www.buzzfeednews.com/article/ellievhall/woman-journey-from-chattanooga-to-isis.
[193] Ellie Hall, How One Young Woman Went From Fundamentalist Christian to ISIS Bride.
[194] USA v. Muhammad Oda Dakhlalla, Factual Basis, Case: 1:15-cr-00098-SA-DAS, United States District Court for the Northern District of Mississippi, 2016.
[195] Offline, the filings note that Young continually asked Dakhlalla when they were going to join ISIL. In a letter to her family, she claimed that 'It was all my planning—I found the contacts, made arrangements, planned the departure," and "I am guilty of what you soon will find out". While in letter between prisons, she wrote to Dakhlalla, she noted that: I know you felt I ruined your life completely… I did. I ruined yours, mine, our

The filings lay out that it was Young that first began to watch pro-IS content on YouTube and showed them to Dakhlalla, including videos of Anjem Choudary and a video of a man, accused of being a homosexual, being thrown from a roof.[196] The FBI also identified Young's Twitter account, which telegraphed her intention to travel, including tweets such as this:

> "@1_modest_woman $$$ for plane tickets" "the only thing keeping me away is $$$ but working all of this overtime will be worth when I am finally there". "I just want to be there :("[197]

Like Bradley, Young also used the Internet to rejoice in the attack in Chattanooga and attempted to reach out to a facilitator who was, in reality, an undercover agent.[198]

It is clear that there are a number of similarities between the actors described above. The first five – Thomas, Yassin, Dais, Coffman, and Muthana – can all be described as highly prolific and potentially influential actors within the online radical milieu. All seven of them regularly posted idealised visions of the caliphate or celebrated IS acts of terrorism. Importantly, although the literature suggests that online, there is a strict gender separation between jihadist actors (Bloom et al. 2017; Pearson 2017), the data here do not suggest that is necessarily the case. Thomas was in contact with three prominent jihadists via direct message; Dais ran a prominent Telegram group dedicated to inspiring lone-actor attacks (it is very unlikely this was populated just by women given the general prohibition against female violence); and Coffman was in direct conversation with a man and other "brothers" in her attempt to facilitate the former's travel. The data suggest that it is possible for female actors to become important and influential members of the radical online milieu, irrespective of gender, influencing both male and female jihadists.

There is a growing literature which researches the topic of female jihadist actors and their use of the Internet. Many scholars have argued that the Internet may provide a unique space for female actors that are not afforded to them in the offline domain. Writing in 2008, Sageman argued that:

> Gender separation among terrorists is starting to disappear because of the Internet… With the semi-anonymity of the Internet, there is no way of keeping them out. (Sageman 2008a, pp.111–112)

---

families'. I single-handedly screwed up everything that could possibly go wrong." The judge accepted this by giving Young and lengthier sentence than Dakhlalla, 12 versus eight years respectively, although Dakhalla did co-operate with authorities more quickly than Young. See: Emma Green, How Two Mississippi College Students Fell in Love and Decided to Join a Terrorist Group, *The Atlantic*, May 1, 2017. Available at: https://www.theatlantic.com/politics/archive/2017/05/mississippi-young-dakhlalla/524751/; USA v. Muhammad Oda Dakhlalla, Factual Basis.

[196] USA v. Muhammad Oda Dakhlalla, Factual Basis.

[197] USA v. Jaelyn Delshaun Young and Muhammad Oda Dakhlalla, Criminal Complaint, Case: 3:15-mj-32-SAA, 2015.

[198] USA v. Muhammad Oda Dakhlalla, Factual Basis.

At a similar time, Bermingham et al. (2009) conducted a social network analysis on a dataset from YouTube, finding that females (and those that did not disclose their gender) scored higher in terms of network density and average communication speed, indicating a potential leadership role for women. These studies suggest that the anonymity of the Internet may encourage gender impersonation which elevates female actors. However, that does not seem to be the case for actors within this sample. Aside from Coffman, there does not seem to be any case of females impersonating males, or even cases in which females do not disclose their gender.

More recently, a study on pro-IS groups on the platform VKontakte also found that female users had superior network connectivity, despite being outnumbered by men. This connectivity was found to potentially benefit the underlying system's robustness and survival (Manrique et al. 2016). Klausen (2015), too, observes the centrality and importance of female actors in IS social media networks. In her study on foreign fighters' Twitter networks, she argues that the prominence of women is striking and that they were mobilised in tactical support roles to an extent far surpassing their involvement in previous jihadist insurgencies. Certainly the qualitative evidence offered above suggests that a number of actors within this sample – particularly Coffman, Thomas, Yassin and Dias – were important players who may have been at the centre of their respective networks.

It would be a mistake, however, to assume that female actors are a monolith; the profiles laid out above suggest that despite showing that they are influential, they exhibit this in different ways and have different motivations. In their study following 93 Twitter accounts of female jihadists for a year, Huey et al. (2017) identify eight overlapping roles: Fan girls;[199] Baqiya members;[200] Propagandists; Recruiters; Muhajirah;[201] Widows; Terrorists;[202] and Leavers.[203] Although there is only a selection of social media posting history, some of these roles can be clearly identified in the women described above. Yassin's posting of memes can be seen as fan girl behaviour, although her re-posting of the kill list is the conduct of a recruiter too.[204] Coffman also exhibits the tendencies of a recruiter in her attempts to arrange the travel of her male partner and the undercover agent,[205] as does Dais' role of providing facilitative information for lone actor attacks.[206] Thomas falls more into the role of propagandist, shown by her history of retweeting the group's and sympathisers' content, such as a picture of a small male child with an AK-47 with the caption:

[199] Fan girls are described as young and enthusiastic about IS because it is cool.
[200] Baqiya translates roughly to "remain". The baqiya family would offer "shoutouts" which help users pick up followers after suspensions.
[201] Females that successfully travelled to the caliphate.
[202] Those charged with terrorism offences.
[203] Those that left the jihadist online milieu.
[204] USA v. Safya Roe Yassin, Criminal Complaint.
[205] USA v. Heather Coffman, Statement of Facts.
[206] USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint.

> "And if I were in Shaam [greater Syria], I wouldn't be pleased till I became soldier of the Islamic State."[207]

As successful travellers, Bradley[208] and Muthana[209] were muhajirah, both tweeting about life in the caliphate and their families. Muthana fulfils the role of widow too, shown by her tweet asking Allah to accept her deceased husband as a martyr.[210] Given the relatively limited information, it is possible that these actors fulfilled more roles; the above examples are merely intended to illustrate the breadth of roles that different influencers may utilise within the milieu.

6.3.3 Peer-to-Peer Communicators

While there are several women within the sample who can be described as influential via their online activities, nine maintained a less overt – but still active – presence. The three women involved in the St Louis/Bosnian plot's funding of Abdullah Ramo Pazara can be described this way. Sedina Unkic Hodzic, Jasminka Ramic, and Mediha Medy Salkicevic all contributed to sending Pazara money in the plot laid out in the previous section analysing financial transactions. The court filings note that all of the actors involved in the plot used Facebook and Email to coordinate efforts and rally support for both Pazara and other fighters.[211] As well as this, the members of the conspiracy were active on Bosnian pro-IS fora.[212] Specifically, the filings note that Ramic contacted Pazara to ask if he needed assistance by email, to which he answered by directing her to the Hodzics[213] and that Salkicevic had a social media presence by the handles "Medy Ummuluna" and "Bosna Mexico" in which she commented on photos uploaded by Pazara from the caliphate, although the filings note that the comment was unusual and that other similar content could not be found on her page.[214] Less is known about Sedina Hodzic's online activity, except that she and her husband were ringleaders and in constant online contact with Pazara.

Several other women fit the mould of those that were active online without necessarily being influencers. Shannon Maureen Conley, for example, who attempted to leave for the caliphate in 2014, met and kept in contact with her unnamed fiancé via social media platforms such as Skype.[215] The filings also omit any evidence of offline social networks,

---

[207] USA v. Keonna Thomas, Criminal Complaint, p.3.
[208] Ellie Hall, How One Young Woman Went From Fundamentalist Christian to ISIS Bride.
[209] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[210] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[211] USA v. Ramiz Zijad Hodzic et al., Government's Opposition to Defendants' Motions to Dismiss the Indictment.
[212] Hughes and Clifford, First He Become American – Then He Joined ISIS, *The Atlantic*, May 25, 2017. Available at: https://www.theatlantic.com/international/archive/2017/05/first-he-became-an-americanthen-he-joined-isis/527622/
[213] St Louis Post-Dispatch, Rockford Woman Pleads Guilty in St Louis Terrorist Funding Case.
[214] USA v. Mediha Medy Salkicevic, Detention Hearing, Case: 4:15-cr-00049-CDP-DDN, United States District Court for the Eastern District of Missouri, 2015.
[215] USA v. Shannon Maureen Conley, Information, Case: 1:14-mj-01045-KLM, United States District Court for the District of Colorado, 2014.

focusing instead on her online activity, potentially suggesting that the Internet had a prominent role in this case.[216] Marie Castelli was part of a closed, invitation only pro-IS Facebook group in which she reposted the above-mentioned "kill list" with the text:

> "A great sister[217] on twitter published addresses of the kafir men who killed sheikh awlaki and his son with the drone[.] [P]raying the mujahadine will send someone for justice[.]"[218]

Another case of peer-to-peer communicators is that of Asia Siddiqui and Noelle Velentzas, who sought to construct a bomb for an attack between 2013 and 2015.[219] Both had some activity within the online jihadist milieu, although neither could be considered influencers. Years previously Siddiqui had written a poem which she posted to Samir Khan's website, which he later published in the e-magazine *Jihad Recollections*,[220] and Velentzas was Facebook friends with jihadist Tairod Pugh[221] and may have been active in pro-IS chatrooms.[222] However, as will be discussed below, the offline connection between the two women played an important role, potentially greater than that of the Internet.

Zoobia Shahnaz is another case that has a clear digital footprint – it is centred around the use of cryptocurrencies – but there is little evidence of her being a prominent voice online. The filings note that she made payments to shell companies in China, Pakistan, and Turkey,[223] which requires some degree of communication. Furthermore, news coverage suggested that she was "radicalised online", but little information is given.[224] There is similarly mixed evidence regarding the case of San Bernardino attacker Tashfeen Malik. It was alleged that her and her husband Rizwan Farook watched Awlaki videos online;[225] may have communicated in private with other individuals;[226] and even that the two may have met on a website which caters to extremists.[227] However, there is little evidence that she was an active member of the jihadist radical milieu. The FBI argued that the couple

---

[216] USA v. Shannon Maureen Conley, Criminal Complaint, Case: 1:14-mj-01045-KLM, United States District Court for the District of Colorado, 2014.
[217] It is possible that this refers to Safya Roe Yassin, although it has not been possible to verify this, not least because of the number of highly connected female actors in this online milieu.
[218] USA v. Marie Antoinette Castelli, Plea Agreement.
[219] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint.
[220] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint.
[221] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint.
[222] Rhonda Schwartz and Randy Kreider, Online Chatter After NYC Terror Arrests: 'Delete Her From Your Phone', *ABC News*, April 6, 2015. Available at: https://abcnews.go.com/International/online-chatter-nyc-terror-arrests-delete-phone/story?id=30124247.
[223] USA v. Zoobia Shahnaz, Indictment.
[224] Harriet Alexander, New York Woman Charged with Sending $85,000 in Bitcoin to Support ISIL.
[225] Maura Conway and Michael Courtney, Violent Extremism and Terrorism Online in 2017: The Year in Review, *Vox Pol*, 2017.
[226] Al Baker and Marc Santora, San Bernardino Attackers Discussed Jihad in Private Messages, FBI Says, *New York Times*, December 16, 2015. Available at: https://www.nytimes.com/2015/12/17/us/san-bernardino-attackers-discussed-jihad-in-private-messages-fbi-says.html.
[227] Karen Greenberg and Seth Weiner, The American Exception: Terrorism Prosecution In the United States - The ISIS Cases- March 2014 - August 2017, *Centre on National Security at Fordham Law*, 2017.

did not make extreme posts on social media,[228] and she even set up a pseudonymous Facebook account on the day of the attack to pledge allegiance to Baghdadi,[229] suggesting she was not active on the platform previously.

Interrelated to the assertion that the online space may provide a unique platform for female actors is the notion that it may also fundamentally change the dynamics of these actors' trajectories. In her study of the British terrorist Roshonara Choudhry, Pearson (2016) makes the point that the Internet allowed Choudhry to eschew the conventional wisdom within jihadist thought regarding violence conducted by women and shop for a scholar who offered alternative agency. This would have been at best very difficult, or at most impossible, had she been at the centre of a radical offline social network given the prevalence of the idea that women should not engage in offensive jihad. The literature on the case of Colleen LaRose – an American woman arrested as part of a cell that planned to kill Danish Cartoonist Lars Vilks – offers a similar picture. Picart (2015) argues that LaRose was able to construct a "gender-bending" representation of herself online, mostly borne out of her own ignorance of Islam and Salafism, which was at odds with a woman's role within the movement. Halverson and Way (2012) also highlight in relation to LaRose, the Internet's ability to proliferate identity fluctuations in the absence of normative social constraints. Both Picart and Halverson and Way also highlight the importance of several offline factors that played a role in LaRose's trajectory.

The notion of the Internet offering a space for female actors to perform their jihadist identity runs throughout many of the actors in the influencer and peer-to-peer communicator category. Conley, for example, has little known connection to a wider milieu, but met and became engaged to her partner online, conducted "research" into Islam on the Internet, and had a stash of Anwar al-Awlaki CDs and DVDs in her luggage.[230] Interestingly, Conley disobeyed her father, who denied her permission to go and marry her fiancée, telling him that she had thought about it and "disagreed with Islam" on this point.[231] This suggests that Conley, without the checks of a conservative social circle, was able to – aided by the Internet – pick and choose which aspects of ideology to adhere. Castelli, too, was active in the closed pro-IS Facebook group and an online forum, participating in discussions and disseminating propaganda, while at the same time, had no connections to offline cells and a friend of hers, upon hearing about her arrest, remarked: 'I thought, they have got the wrong person, there's no way she can be like that.'[232] Both Conley and Castelli exhibited strange offline behaviours which alerted

[228] Al Baker and Marc Santora, San Bernardino Attackers Discussed Jihad in Private Messages, FBI Says.
[229] USA v. Enrique Marquez Jr, Criminal Complaint.
[230] USA v. Shannon Maureen Conley, Criminal Complaint.
[231] USA v. Shannon Maureen Conley, Criminal Complaint.
[232] Michael Monks, Friend Who Photographed Her Surprised by Maysville Woman's Arrest, *River City News*, September 18, 2016. Available at: https://www.rcnky.com/articles/2016/09/18/friend-who-photographed-her-surprised-maysville-womans-arrest.

others to their presence – at a church[233] and courthouse[234] respectively – but the filings in both cases suggest that they both lived quite distinct lives online and offline.

Many of the filings from actors in the influencer category also draw on the dichotomy of a substantially different constructed identity between their online and offline lives. Coffman's defence counsel notes that she grew up in a protective household and was 'isolated from the real world' and 'the internet became her social outlet.'[235] In Thomas' case, the US Government prosecutors highlighted that she was "living a double life"; one of a quiet and hard-working mother who stayed out of trouble, and one of "Fatayat Al Khilafah", an online persona with a large following, an outspoken personality, spreading violent jihadi propaganda, who was also a close associate of several known jihadi fighters.[236] Yassin too, seemingly lived a double life. When she was arrested one neighbour remarked that it was the first time they had seen her in months, while another had never seen her before; a reporter said that it was difficult to find people that knew her because of her reclusive nature.[237]

Dais' defence counsel also argued that she was a stay-at-home mother who is strapped for cash and whose actions may have been driven by an attempt to seek out friendship and romantic connections.[238] Finally, coverage of Muthana's case dwells on her Twitter alter-ego and how different it was to her offline persona. A friend from Alabama told a journalist that 'you would never have thought that she was anything other than a quiet, shy girl'[239] and that she portrayed herself to be more religious on social media than she actually was, giving the example of Muthana claiming to dress modestly and conservatively when online while wearing Western-style clothes offline.[240] Her friend suggested that this ultra-religious alter-ego was responsible for her influence within jihadist Twitter; 'what she lacked in her personality she would make up for on Twitter.'[241] In an interview with a journalist, Muthana seemed to agree with this, stating that prior to her travel 'I literally isolated myself from all my friends and community members the last

[233] USA v. Shannon Maureen Conley, Criminal Complaint.
[234] Mike Levine, Ahead of 9/11 Anniversary, FBI Arrests Kentucky Woman for Allegedly Promoting ISIS-Inspired Attacks, *ABC News*, September 9, 2016. Available at: https://abcnews.go.com/US/abc-ahead-911-anniversary-fbi-arrests-kentucky-woman/story?id=41975069.
[235] USA v. Heather Coffman, Defendant's Position on Sentencing, Case 3:15-cr-00016-JAG, United States District Court for the Eastern District of Virginia, 2015, p.6.
[236] USA v. Keonna Thomas, Government's Sentencing Memorandum.
[237] Thomas Gounley, Neighbors Never Saw Her. But Buffalo Woman Arrested by FBI was "Well Known…in the ISIS Twitter Scene, *Springfield News Leader*, February 25, 2016. Available at: https://eu.news-leader.com/story/news/crime/2016/02/25/safya-roe-yassin-well-known-isis-twitter-scene-fbi-arrested-buffalo-missouri-terrorism-woman/80621154/.
[238] John Diedrich, A Cudahy Woman Charged with Promoting ISIS and Suggesting Attacks on Festivals, Churches Held on Bail, *Milwaukee Journal Sentinel*, June 15, 2018. Available at: https://eu.jsonline.com/story/news/crime/2018/06/15/cudahy-mom-charged-promoting-isis-attacks-held-without-bail/702851002/.
[239] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[240] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[241] Ellie Hall, Gone Girl: An Interview with An American in ISIS.

year I was in America'.[242] This is particularly striking given, as described above, her parents forbade her from even using social media.

It is important not to sample the dependant variable; there are many male actors that the filings suggest were living a double life, too. The court filings in the case of Ali Shukri Amin, the owner of the influential @AmreekiWitness Twitter account, paint the picture of an immature social recluse whose disability prevented him from leaving the house and was emboldened by the jihadist online milieu.[243] Similarly, Akhror Saidahkmetov's poor English-language skills and lack of friends in New York led to a withdrawal from school and social life, which caused him to turn to the Internet.[244] Interviews with the family and friends of Christopher Lee Cornell portray him as a 'momma's boy who never left the house'[245] who lived a 'fantasy life behind a computer screen.'[246] All three of these actors exhibit a degree of social isolation for reasons other than gender which was overcome by online activity – this theme will be discussed in the next section.

To be clear, none of the female actors described above opted for violence, as in the cases of Choudhry and LaRose. However, the Internet has still offered opportunities for empowerment within the movement. As noted above by Klausen, 'online, women are mobilized as partisans and in tactical support roles to an extent far surpassing their involvement in any previous jihadist insurgency' (Klausen 2015, p.16). Similarly, Melegarou-Hitchens et al. note that of the IS travellers, 'women play an outsized role and are heavily involved in creating and cultivating recruitment networks' (Meleagrou-Hitchens et al. 2018, p.86). Even in cases that do not involve direct violence, the Internet offers a platform which can empower women to – in Pearson's (2016) words – perform a less restricted gender identity.

However, the Internet is neither necessary nor sufficient for female empowerment, as can be seen in the case of Noelle Velentzas and Asia Siddiqui. Unlike many of the influencers above, the filings suggest that online communication seemed peripheral to their plot. The two relied on the Internet for planning and downloading multiple copies of *Inspire* magazine as well as *The Anarchist Cookbook* for bomb-making instructions. However, the two women and the undercover agent formed a seemingly tight knit group of three females who were both aware and acted beyond the gender roles that the offline jihadist community would usually allow for them. Velentzas, in particular, expressed a repeated thirst for violence, like when she pulled a concealed knife from her bra and asked the

[242] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[243] USA v. Ali Shukri Amin, Defendant's Sentencing Memorandum.
[244] USA v. Akhror Saidahkmetov, Defendant's Sentencing Memorandum, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York, 2017.
[245] Kimball Perry and Patrick Brennan, Father: Terror Plot Suspect Was A 'Momma's Boy', *Cincinnati.com*, January 23, 2015. Available at: https://eu.cincinnati.com/story/news/crime/crime-and-courts/2015/01/14/fbi-cincinnati-man-plotting-us-capitol-attack-arrested/21770815/.
[246] Dan Sewel, Attorneys: Tri-State Man Behind Terror Plot Now Rejects "Radical Islam" Wants Lighter Sentence, *WPCO Cincinnati*, November 30, 2016. Available at: https://www.wcpo.com/news/local-news/hamilton-county/cincinnati/defense-urges-lighter-sentence-for-plot-to-attack-us-capitol.

other two: 'Why we can't be some real bad bitches?'[247] or when she described her intended attack as: "This is what it looks like. 'In your face, nigger. Oh, you're dead'.[248] Similarly, when purchasing bomb-making equipment from Home Depot, Velentzas told the undercover agent 'Some women like to look at clothes. I like to look at electric equipment'.[249] Both repeatedly made reference to their gender, but neither saw an inherent contradiction in conducting a terrorist attack. Importantly, unlike the case of Roshonara Choudhry as laid out by Pearson (2016), breaking these gender norms, at best, played out only partially online and the two actors' offline relationship clearly played an important role.

6.3.4 Offliners

In contrast to the influencers and peer-to-peer communicators, several women had little-to-no online communication, with some even taking steps to remove themselves from the online domain. One example of this is Yusra Ismail, who travelled from Minneapolis to Syria in December 2014.[250] Not only is there a very limited trail of online evidence of Ismail's trajectory, but her sister told journalists that she deactivated her Facebook account months ago, conceding that she may be active on other platforms.[251] Relatives suggest that she had been targeted by recruiters,[252] however it is likely that this was offline. Around two years before travel, she switched mosques and began attending the Dar al Farooq Islamic Centre, the same Mosque as several other Minnesotan travellers, including Abdi Nur, Abdullahi Yusuf, and the Farah brothers.[253] It is worth noting that there is no evidence directly linking Ismail to either the first or second wave of Minnesotan travellers, but does suggest that the venue may have hosted individuals with radical ideologies.

Only scant online trails can be found for Zakia Nasrin, too, who successfully travelled to Syria with her husband Jaffrey Khan and brother Rasel Raihan in July of 2014.[254] She met her husband online and she immediately began to show more conservative behaviour after they married.[255] There is also evidence that he was controlling her social media, shown by the fact that in a conversation with Nasrin's high school friend on Facebook, Khan interjected with:

---

[247] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint, p.12.
[248] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint, p.20.
[249] USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint, p.26.
[250] USA v. Yusra Ismail, Criminal Complaint, Case 0:14-mj-01047-JSM, United States District Court for the District of Minnesota, 2014.
[251] Laura Yuen, Gone to Syria: Family Fears Woman Latest Minnesotan Drawn to War-torn Region, *MPR News*, September 11, 2014. Available at: https://www.mprnews.org/story/2014/09/11/muslim-woman-disappears-syria.
[252] Paul McEnroe, St Paul Woman Charged with Stealing Passport to Travel to Syria, *Star Tribune*, December 3, 2014. Available at: http://www.startribune.com/st-paul-woman-charged-with-stealing-passport-to-travel-to-syria/284520161/.
[253] Sasha Aslanian, Laura Yuen and Mukhtar M. Ibrahim, Called to Fight: Minnesota's ISIS Recruits, *MPR News*, 25 March 2015. Available at: https://www.mprnews.org/story/2015/03/25/minnesota-isis#yismail.
[254] Richard Engel, Ben Plesser, Tracy Connor and Jon Schuppe, The American: 15 Who left the US to Join ISIS.
[255] Meleagrou-Hitchens, Hughes, and Clifford, The Travelers.

> Zakia got married. I'm her husband lol… Zakia talks about you a lot and misses you as you were her best friend, so I told her to contact you, but she's too shy/embarrassed. So I convinced her to at least send you a message on facebook, and she agreed on the condition that she doesn't have to look at your reply or anything lol.[256]

Similarly little can be found regarding Tania Georgelas who travelled with her husband and children in August 2013.[257] She sometimes posted pseudo-political content roughly aligned with jihadist thought:

> You guys (meaning Americans) need to stop supporting democracy, and just make Ron Paul your king.[258]

Beyond this, and the statement that she "supported" her husband on social media,[259] there is little to suggest she was an active participant in the online jihadist milieu.

It is important to note the actors who do not seem to be active participants in the online jihadist community for several reasons. Firstly, to reiterate that pathways towards terrorism are heterogeneous, a finding consistent across several studies (Vidino et al. 2017; Klausen 2016a; Gill et al. 2015; Horgan et al. 2016). Just as the findings above show that the women who actively maintain an online presence can play different roles within the jihadist community, there are also a number that barely engage online at all.

Secondly, although the Internet can afford female actors the opportunity to perform a less restricted gender identity, it does not mean that this is a certainty. Much of the literature still suggests that the most important role for females in the Salafi-jihadi movement is to be a wife and stay-at-home mother first and foremost (Saltman and Smith 2015; Europol 2019b). It is important to note that, according to a report by Europol, this too can be seen as empowerment. They suggest that for "jihadi feminism", in contrast to Western feminism and Islamic feminism, it is important that gender roles are not blurred because they are subject to divine reference. On this view, constructing a conservative and traditional gender role of being primarily a wife and mother empowers females to live life as God intends (Europol 2019b). Pearson (2019) also makes this point, noting that IS produces a narrative to sell its own vision of female empowerment and frames it in competition to the immoral and secular understanding that pertains in the West today.

Thirdly, it is worth noting that all three of the actors with a minimal presence were all successful in travelling to the caliphate. The quantitative findings of Chapter 5 found a significant and inverse correlation between online behaviours and the likelihood of

---

[256] Richard Engel, Ben Plesser and Tracy Connor, An American ISIS Cell: The Story of 3 U.S. Recruits, *NBC News*, May 19, 2016. Available at: https://www.nbcnews.com/storyline/isis-uncovered/american-isis-cell-story-3-u-s-recruits-n573831.

[257] Graeme Wood, An American Climbing the Ranks of ISIS, *The Atlantic*, January 25, 2017. Available at: https://www.theatlantic.com/magazine/archive/2017/03/the-american-leader-in-the-islamic-state/510872/.

[258] Graeme Wood, An American Climbing the Ranks of ISIS.

[259] Graeme Wood, An American Climbing the Ranks of ISIS.

success. Influencers like Thomas, Yassin, and Dias made themselves easily identifiable by posting on open social media platforms, and the criminal cases against peer-to-peer actors like the three Bosnians was made easier by the online trail left. It is also possible that staying quiet or removing themselves from the online radical milieu was advised by recruiters for this reason. Of course, the success of an event relies on more than simply staying off social media – Muthana was able to maintain an active presence and travel successfully. Factors such as offline social networks and when the actor attempts to travel certainly play an important role too.

6.3.5 Synthesis

The role of gender in violent extremism remains an understudied topic, particularly in the online domain. Conway (2016a) notes that the role and influence of women in violent extremist cyberspace remains largely unknown and when the topic is addressed, women are often discussed only as a motivator for their male counterparts. Similarly, Pearson argues that gender is a key gap for research into violent extremism online and that 'studies on how gender factors in online radicalization are still in their infancy' (Pearson 2017, p.4). It is not difficult to see why this imbalance persists as this and other research identifies that terrorists are primarily men; in fact, it remains one of the only reliable predictors of engagement (Bouhana 2019). However, as this chapter establishes, there is much that can be learned from analysing female participation in online extremist milieus.

This section is fundamentally about space and the ways in which women use it to carve out their emerging radical identity. Constant comparison of the women in this sample shows that, for some, the Internet acted as a space for them to break the socially mandated gender boundaries – like Thomas who was in contact with high ranking and renowned IS members online. For others, it went even further, like both Coffman and Dais who broke gender roles by pretending to be men online. For actors like Muthana, it was an opportunity to disobey her overbearing parents to create status in a community. In essence, it affords a platform to achieve personal agency by communicating with others. This is in line with the previous section on radical content; rather than a cause-and-effect radicalisation dynamic, the Internet provided these women with a venue to be social and explore their ideological development. Much like the use of the Internet to create avatars of the "Good Muslim" or to shitpost, for women, acting online may have offered the opportunity for them to construct a fundamentally different persona.

However, women are not a monolith. Pearson and Winterbotham (2017; p.2) argue, 'the reasons for Western female radicalisation to [IS] are complex', and just as there are differences between female and male actors, they also have different criminogenic factors as well as psychological needs and gratifications to other women. While several females in the sample were able to utilise the Internet to become influential within the jihadist online radical milieu, within this group several different roles are constructed, such as that of fan girl, recruiter, and muharjrah. Furthermore, many women used the Internet in a less prominent way than the influencers, but there is still reason to suggest that it may have provided a platform for them to perform a less restricted gender identity than they

could have offline. However, cases like that of Velentzas and Siddiqui show that this can be done without a heavy reliance on the Internet. Finally, some deliberately eschewed the Internet, possibly because they did not seek a less restricted gender identity, or perhaps out of pragmatism. These cases highlight the heterogeneity of different pathways to terrorism, a finding consistent across several studies (Vidino et al. 2017; Klausen 2016a; Gill et al. 2015; Horgan et al. 2016). While it may be tempting to treat "women" as a homogenous block, the data presented here suggest this is not the case.

Grounded Theory

2. *The Internet can provide a platform for female actors to construct a less restricted female identity than would otherwise be possible within the Salafi-jihadist movement.*

6.4 Online Only Trajectories and the Buyers' Market of the Internet

6.4.1 Introduction

Chapter 5 found that, across the whole sample of 201, actors used the Internet heavily but also tended to act in both domains. However, when coding the previous section on gender, the data showed that several female actors relied heavily on the Internet, which gave them a space to perform a less restricted gender identity. With that in mind, I deemed it instructive to analyse those at the heavy-usage end of the spectrum to assess whether there are instances in which actors engaged exclusively online – from their first involvement within the radical milieu to their eventual activity or arrest. After coding the data descriptively, they were then selectively coded into emergent themes such as entry points, online behaviours, and offline behaviours, which were compared against each other.

Line-by-line analysis suggests that there are only five cases – three of which are females discussed in the previous chapter – which can be ascribed the possibility of an online only trajectory, and these cannot even be confirmed due to the limitations of open-source data. In at least four of these cases, the theme of social isolation emerges from the data; individuals were described by onlookers as being removed from day-to-day society and therefore used the Internet heavily as part of their radicalisation trajectory. Theoretically sampling outwards towards the wider sample, this is a theme that occurs elsewhere too – many terrorists seem to be isolated at the point in which they use the Internet to engage with propaganda or connect with co-ideologues. This suggests that, for a small number at least, social isolation may act as a stressor which facilitates online radicalisation. However, two important caveats should be noted. Firstly, these cases are few in number compared to individuals that do engage face-to-face, or are part of society, suggesting that this is only a potential dynamic for *some*, and secondly, the direction of this relationship is not clear – that is to say, it is not clear whether isolation causes individuals to engage more in the radical online milieu, or whether engaging in it causes actors to remove themselves from their other social groups.

Given that the burden of evidence may be unrealistically high for online only trajectories, I decided to expand on this analysis by theoretically sampling the whole cohort for the entry points into the radical milieu as a means of understanding whether the Internet provided the first steps into the movement. There are more actors that use the Internet as an entry point – 17 in total – and those that do have several different motivations for engaging online. This includes individuals seeking a more fulfilling religious experience; those who moved sideways from conspiracy theory communities; actors seeking to extend their university learning; those with an existing interest in Middle East conflicts; and individuals with predispositions that may have been exacerbated by radical content.

Taken together, this section points to the Internet as a tool for individuals to fulfil a range of needs that they may be unable to fulfil in other parts of their life. In this sense it should be considered a facilitative platform which operates in a less hierarchically structured and regulated manner, which allows individuals the freedom to pick and choose their communities, akin to a buyers' market.

6.4.2 Online Only Trajectories

Keonna Thomas

As highlighted in the previous section, Keonna Thomas was notable for maintaining an active online presence which included online peer-to-peer conversations with a number of notable jihadists: Abdullah el-Faisal, Mujahid Miski, and Shawn Parson.[260] The defence counsel's sentencing memorandum notes that Thomas, who was unemployed and lived with her mother and two small children experienced emotional and physical isolation, which she fulfilled by turning to the Internet, which in turn led to her falling 'prey to the promises made by young ISIL acolytes about a religious utopia in Raqqa.'[261] Her lawyers also suggested that in her loneliness and desperation for social interaction, she spent 13 hours or more per day on jihadist online fora after receiving her first computer in 2010, which led to her becoming an outspoken supporter of Islamic fundamentalism.[262]

The prosecutors also paint the picture of a woman living a double life, on one hand quiet and reserved in the offline sphere and on the other an influential member of the jihadisphere, spreading propaganda and operational advice for those travelling to Syria.[263] In Thomas' case, it appears that her radical behaviour did not leave the confines of her own home – she booked her travel from Philadelphia to Barcelona with the intention of travelling to Istanbul by bus, but the Government executed a search warrant of her house days before her scheduled travel.[264] Her heavy usage of the Internet, taken

[260] USA v. Keonna Thomas, Criminal Complaint.
[261] USA v. Keonna Thomas, Defendant's Sentencing Memorandum, pp.3-4.
[262] Jeremy Roebuck, North Philly Woman Gets 8 Year Term for Plan to Leave Kids, Marry IS Soldier, *The Inquirer*, September 6, 2017. Available at: http://www.philly.com/philly/news/pennsylvania/philadelphia/north-philly-mom-gets-8-year-term-for-plan-to-leave-kids-marry-isis-soldier-20170906.html.
[263] USA v. Keonna Thomas, Government's Sentencing Memorandum.
[264] USA v. Keonna Thomas, Government's Sentencing Memorandum.

with reports of social isolation, description of leading a double-life, and a lack of evidence to suggest her behaviours spilled over into the offline domain, suggest that she is a strong candidate to be seen as an online only trajectory.

Safya Roe Yassin

There are strong parallels between Thomas' case and that of Safya Roe Yassin. As with Thomas, Yassin's filings describe her as a socially isolated mother living with a parent. In cross-examination in court, her father noted that she had been living with him for around eight years after she became disabled; that she was unemployed; and that she home-schooled her son after she pulled him out of school after facing Islamophobic abuse.[265] Reporting highlights her isolation, too. When she was arrested neighbours commented that they had not seen her in months and the newspaper even suggested that they could not find anyone who knew her to interview because of her reclusive nature.[266] Similarly, when asked by journalists, a spokesman of the local mosque said that he did not know her and that she was unlikely to have been well-known in the community if she was not in contact with members of the congregation.[267] However, within her own home, she maintained an active and influential presence on Twitter using a number of different handles,[268] as laid out in the previous section.

Importantly, her presence as an active voice online pre-dates her involvement with IS; she was a member of a number of communities expounding different conspiracy theories, including the belief that vaccines cause autism, "chemtrails", and anti-genetically modified foods.[269] Given the link drawn between conspiracy theories and involvement in extremism (for example, see: Bartlett and Miller 2012; Berger 2017), it is possible – although not explicitly stated – that the Internet was an entry point for Yassin, or at least primed her for the radical online milieu. As with Thomas, it seems she never exhibited any offline behaviours outside her home. She was arrested for disseminating the "kill list" online and she was apprehended at her residence after a brief standoff in which she claimed to have a knife.[270]

Hoda Muthana

The case for Hoda Muthana having an online only trajectory is even starker than for Yassin and Thomas. As noted in the previous section, Muthana successfully travelled to the caliphate in 2014 after maintaining an active presence on Twitter.[271] In an interview

[265] USA v. Safya Roe Yassin, Transcript of Hearing on Initial Appearance, Case No. 16-03024-01-CR-S-MDH, United States District Court for the Western District of Missouri Southern Division, 2016.
[266] Thomas Gounley, Neighbors Never Saw Her. But Buffalo Woman Arrested by FBI was "Well Known…in the ISIS Twitter Scene.
[267] Thomas Gounley, Neighbors Never Saw Her. But Buffalo Woman Arrested by FBI was "Well Known…in the ISIS Twitter Scene.
[268] USA v. Safya Roe Yassin, Criminal Complaint.
[269] Katie Zavadski, The American Anti-Vaccine Mom Turned ISIS Superstar.
[270] USA v. Safya Roe Yassin, Transcript of Hearing on Initial Appearance.
[271] Meleagrou-Hitchens, Hughes, and Clifford, The Travelers.

with her father, he affirmed that she was subject to his conservative "old country" rules in which she and her sister were not permitted to speak to anyone outside of the family or use social media.[272] Both her father and her classmates described Muthana as someone who did not have any friends in real life, which she confirmed by saying that she isolated herself from those she knew, including her local Muslim community.[273]

A key part of her radicalisation was her father's graduation gift of a cellphone, which was explicitly stated by Muthana as her gateway into the radical online milieu. First, she began watching lectures of scholars on YouTube, which she says influenced her much more than the preachers in her local community, then, she set up a secret Twitter account which generated thousands of followers.[274] As noted in the previous section, those that knew her commented on the sharp distinction between her online and offline personas, with one suggesting that she crafted an online identity to appear more religious than she was in reality.[275] This case shows a clear trajectory from social isolation – enforced by her father, to using the Internet and finding radical content, to Muthana's eventual activity, all of which seemingly took place online.

Mohamed Khweis

Mohamed Khweis successfully travelled to the caliphate in 2015, before being captured by Kurdish forces and was eventually charged with, and found guilty of, providing material support to a foreign terrorist organisation.[276] The filings note that Khweis began conducting online research relating to IS in about 2015 and that he frequently watched their propaganda videos,[277] as well as maintaining multiple Facebook and Twitter accounts for communicating with co-ideologues,[278] and even used the TOR browser to use the web anonymously.[279]

Meleagrou-Hitchens et al. note that Khweis 'reportedly told no one of his plans before he left, was largely influenced by his online activities, [and] was not involved in any known physical jihadist networks in the US,'[280] making him an outlier compared to the others that travelled from the US to the caliphate. Khweis travelled alone via London, even attempting to contact a member of al-Muhajiroun, who did not respond to his online message, to Turkey, where he continued to use social media to attempt to find a way into the caliphate, in which he was eventually successful.[281] Although Meleagrou-Hitchens et

[272] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[273] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[274] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[275] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[276] USA v. Mohamed Jamal Khweis, Criminal Complaint, Case 1:16-mj-00213-JFA, United States District Court for the Eastern District of Virginia, 2016.
[277] USA v. Mohamed Jamal Khweis, Criminal Complaint.
[278] USA v. Mohamed Jamal Khweis, Government's Amended Trial Exhibit List (June 1, 2017), Case 1:16-cr-00143-LO, United States District Court for the Eastern District of Virginia, 2017.
[279] USA v. Mohamed Jamal Khweis, Government's Sentencing Memorandum, Case 1:16-cr-00143-LO, United States District Court for the Eastern District of Virginia, 2017.
[280] Meleagrou-Hitchens et al., The Travelers, p.63.
[281] Meleagrou-Hitchens et al., The Travelers.

al. note that 'there may never be a fully comprehensive account of what drove Khweis to join the group', his online activities and the positive affirmation that there is no evidence linking him to offline recruitment networks suggest there is a good possibility that he had an online only trajectory.

Zulfi Hoxha

Another candidate for an online only trajectory is Zulfi Hoxha, who, like Khweis, successfully travelled to the caliphate in 2015, but unlike Khweis, he rose through the ranks, appeared beheading prisoners in propaganda videos, and is thought, if alive, to be a senior commander in IS.[282] Hughes et al. note that Hoxa's case highlights the importance of jihadist recruitment networks within the United States and that he made these connections via the Internet which was able to help facilitate his travel to Syria.[283] They discuss how he met David Wright via the gaming website Steam between 2010 and 2014, were members of radical PalTalk communities "The Solution for Humanity" and "Road to Jannah," and kept in contact on Skype.[284] Wright and his uncle Usaamah Rahim both helped Hoxha travel with Rahim selling his laptop to raise funds for Hoxha's plane tickets and the two providing all important contacts with facilitators to aid his travel – Rahim was even in conversation with Junaid Hussain about Hoxha, suggesting the he may have helped the process himself.[285]

Hughes and colleagues do not offer evidence that this network activity spilled over into the offline domain before Hoxha's eventual travel and repeatedly reinforce the importance of the Internet.[286] The reporting around the case also highlights his isolation from the social world – those that knew him commented that "he was so shy. He never talked to people"[287] and that he became disillusioned with his mosque several years previously.[288] In contrast, he was vociferous online, getting into arguments on Twitter with the State Department's Think Again, Turn Away strategic communications campaign.[289] Ultimately, as Hughes and colleagues point out, little is known about

[282] Hughes et al. A New American Leader Rises in ISIS.
[283] Hughes et al. A New American Leader Rises in ISIS.
[284] Hughes et al. A New American Leader Rises in ISIS.
[285] Hughes et al. A New American Leader Rises in ISIS.
[286] Hughes et al. A New American Leader Rises in ISIS.
[287] Rebecca Everett, Before Joining ISIS in Syria, Jersey Shore Man Was a Shy 'Closed Person', *NJ.com*, January 20, 2018. Available at: https://www.nj.com/atlantic/index.ssf/2018/01/nj_man_who_became_isis_commander_was_shy_closed_pe.html.
[288] Ted Greenberg and Brian McCrone, 'I Hate You, Americans': Co-Worker, Friend Recall ISIS 'Senior Command' From Jersey Shore, *NBC News*, January 18, 2018. Available at: https://www.nbcphiladelphia.com/news/local/I-Hate-You-Americans-Co-Worker-Friend-Recalls-ISIS-Senior-Commander-From-Jersey-Shore--470009243.html.
[289] Craig McCoy, Dylan Purcell and Jan Hefler, From Atlantic City High to ISIS: The Path of a Homegrown Terrorist, *Philadelphia Inquirer*, January 19, 2018. Available at: http://www2.philly.com/philly/news/nation_world/american-isis-commander-atlantic-city-margate-zulfi-hoxha-2-20180119.html.

Hoxha's background,[290] but the reliance on the Internet in forging a recruitment network, taken with a lack of evidence of any offline activity prior to his travel and testimony that he was isolated and withdrawn suggest Hoxha may have only acted online.

When comparing these five cases, the theme of social isolation repeatedly emerges from the data. Four of the five individuals were described, either by prosecutors, themselves, or acquaintances as being isolated from wider society. Isolation has often been described as a potential radicalisation dynamic. For example, in their case study based research, both Gartenstein-Ross and Grossman (2009) and Silber and Bhatt (2007) find that individuals who are radicalising isolate themselves from wider society which can push them towards radical ideologies. This is particularly the case for research into lone actor terrorists; Nesser (2012) argues that social isolation is a key vulnerability, while Peddell and colleagues' (2016) interview research with practitioners also finds this to be an important factor. This is relevant to this section because each of the five actors identified above attempted to execute their plots alone, either as lone actor with no direction or a solo actor with direction.

For individuals that are socially isolated, the potential affordances of the Internet are quite clear. Theoretical online radicalisation research has posited it as both an outlet to isolation and a vicious cycle in which individuals become more so. Torok (2013) argues that self-imposed isolation is a key mechanism of online radicalisation, providing insulation from external influences and outside ideas, while normalising extreme behaviours. Neo's (2016) multi-stage model of online radicalisation also points towards this dynamic, suggesting that individuals can become "trapped" within deviant online communities and withdraw from the outside world because their new beliefs are at odds with their friends and families'. Post, McGinnis, and Moody (2014) create a typography of a "lonely romantic" terrorist, who is socially isolated but wishes to eschew this to become part of a wider group or movement. This individual is vulnerable to recruiters' messages on social media who are able to present a romanticised notion of revolution, providing a sense of meaning to their life.

Given this recurring theme, it is instructive to theoretically sample outwards to other individuals that may have experienced social isolation and heavy Internet usage, even if they did eventually have some offline antecedent behaviours. Islam Natsheh is a clear example of this, who according a family friend fell into a depressive state and refused to leave his room and instead engaged with IS propaganda and sympathisers.[291] Several individuals, such as Sayfullo Saipov,[292] Clark Calloway,[293] and Aziz Sayyed,[294] lacked face-

[290] Hughes et al. A New American Leader Rises in ISIS.
[291] USA v. Islam Natsheh, Defendant's Sentencing Memorandum.
[292] Mansur Mirovalev and Eric Levenson, NY Terror Suspect Planned to Return to Uzbekistan, Sister Says, *CNN*, November 5, 2017. Available at: https://edition.cnn.com/2017/11/04/us/ny-terror-attack-suspect-sister/index.html.
[293] USA v. Clark Calloway, Criminal Complaint.
[294] Erin Edgemon, Alabama Student Pleads Guilty in ISIS Plot, Obtaining Bomb Making Materials, *AL,* March 8, 2018. Available at: https://www.al.com/news/birmingham/2018/03/alabama_student_pleads_guilty.html.

to-face social connections and engaged with radical content via social media. Others were described by loved ones or acquaintances as either lost,[295] lonely,[296] reserved,[297] or isolated[298] whilst simultaneously acting within the online radical milieu. Therefore, there may be a relationship between some actors experiencing isolation and taking a step further towards an act of terror via the Internet, as theorised by Torok (2013), Neo (2016), and Post, McGinnis, and Moody (2014).

Although this section posits a relationship between social isolation and increased engagement in the radical online milieu, it should be noted that there is little reason to believe the social isolation is the causative factor in individuals' radicalisation; in each of the cases there are a range of factors at play. Moreover, the direction of the relationship is often not clear, which is to say, the data do not elaborate as to whether isolation causes an individual to engage with online radical content, or whether engaging with such content leads to an actor isolating themselves from their peers.

Despite this finding, it should be reiterated that these individuals represent only a small minority of the total number of terrorists in the sample. Compared to the five potential "online only" cases, 167 were deemed to have engaged either in an offline network with co-ideologues or to have learned about or planned their event offline, or both.[299] There are a number of different ways in which this occurred, such as those that trained offline by going to a gun range;[300] hiring out a truck in advance of a vehicle-borne attack to practice;[301] or underwent physical exercise in groups to prepare for travelling to Syria.[302] Actors also went abroad and came into contact with recruitment networks;[303] met up in

[295] Jenny Deam, Colorado Woman's Quest for Jihad Baffles Neighbours, *LA Times*, July 25, 2014. Available at; http://www.latimes.com/nation/la-na-high-school-jihadi-20140726-story.html#page=1.
[296] Patrick Brennan, Father: Terror Plot Suspect Was A 'Momma's Boy', Cincinnati.com, January 14, 2015. Available at: https://www.cincinnati.com/story/news/crime/crime-and-courts/2015/01/14/fbi-cincinnati-man-plotting-us-capitol-attack-arrested/21770815/.
[297] Joe Jackson, Terror Suspect Called a Quiet Loner, Wall Street Journal, February 27, 2015, Available at: https://www.wsj.com/articles/terror-suspect-called-a-quiet-loner-1425089215.
[298] CBC News, Canadian Convicted of Terrorism in US asks for 2nd Chance, March 3, 2018. Available at: http://www.cbc.ca/news/world/canadian-convicted-of-terrorism-in-u-s-asks-for-2nd-chance-1.4561306.
[299] This means that for 29 actors that did not exhibit radical behaviours in the offline domain, not enough evidence could be found to include them as a possible candidate for an online only trajectory (167 that acted offline, 5 potential online only candidates, and 29 with not enough information to make a firm judgement, equalling the 201 actors in this sample.)
[300] For example: Rizwan Farook and Tashfeen Malik - Pete Williams and Halismah Abdullah, FBI: San Bernardino Shooters Radicalized Before They Met, *NBC News*, December 9, 2015. Available at: https://www.nbcnews.com/storyline/san-bernardino-shooting/fbi-san-bernardino-shooters-radicalized-they-met-n476971; Aziz Sayyed, USA v. Aziz Ihab Sayyed, Case 5:18-cr-00090-AKK-HNK, United States District Court for the Northern District of Alabama, 2018; Neleash Mohamed Das, Criminal Complaint.
[301] For example: Sayfullo Saipov – USA v. Sayfullo Saipov, Criminal Complaint, Case 1:17-mj-08177, United States District Court for the Southern District of New York, 2017.
[302] For example: Joseph Jones and Edward Schimenti - USA v. Joseph Jones and Edward Schimenti, Criminal Complaint.
[303] For example: Mohamed Jalloh – USA v. Mohamed Bailor Jalloh, Criminal Complaint, Case 1:16-mj-00296-TCB, United States District Court for the Eastern District of Virginia, 2016.

order to plan travel to the caliphate;[304] or sought spiritual authority in person.[305] Many cases within this sample have heavy digital footprints, but there are very few that do not spill over in some way into the offline domain.

This is, for the most part, in line with the previous literature on the topic. In their study of "online radicalisation", von Behr et al. (2013) test 15 case studies against five hypotheses, including that the Internet was replacing the need for physical contact. They reject this, noting that 'in all our cases the so called offline world played an important role in the radicalisation process. The subjects had offline contact with family members or friends who shared their beliefs' (von Behr et al. 2013, p. 33). Gill et al. (2015) also note this when discussing Roshonara Choudhry's lack of physical network leading to her decision to attack Stephen Timms, suggesting that her case is an outlier and that the vast majority of terrorists in their sample act in both domains. Reynolds and Hafez's (2017) study on foreign fighters from Germany offers a similar picture, finding that only four actors in their sample of 99 could be confirmed as being driven by social media. To further strengthen the argument of the relationship between females and their constructed online identity, 'all four of these cases involved women who were recruited through undisclosed social media contacts' (Reynolds and Hafez 2017, p.19).

Despite a lack of empirical evidence, research has previously posited a possibility of online only trajectories becoming the new normal. For example, in their *Homegrown Islamic Extremism in 2013* report, the ADL find that: 'Face-to-face interaction with terrorist operatives is no longer a requirement for radicalization. Individual extremists, or lone wolves, are increasingly self-radicalizing online with no physical interactions with established terrorist groups or cells' (Anti-Defamation League 2014, p.1). This is markedly similar to Sageman's claim that 'face-to-face radicalization has been replaced by online radicalization' (Sageman 2008b, p.41). The findings offered above do not support claims that this is happening on a significant scale. Other research has been more cautious, such as a report on foreign fighters for the UN-CTED, which found that direct personal contact was required in most cases, but that 'some Member States have reported instances of Internet-only radicalization or so-called "self-indoctrination" (UN CTED 2015, p.18). Similarly the Institute for Strategic Dialogue find that 'there are few examples of individuals radicalising entirely online, but there are signs that this could increase over time' (Institute for Strategic Dialogue 2011, p.1), although they too, stress the importance of offline networks. Meleagrou-Hitchens and Kaderbhai note that:

> The vast majority of scholars argue that, while the Internet plays a facilitating role, in most cases the individual must still be in contact with real-world

[304] For example: Ali Shukri Amin and Reza Niknejad – USA v. Ali Shukri Amin, Position Of The United States With Respect To Sentencing, Case 1:15-cr-00164-CMH, United States District Court for the Eastern District of Virginia, 2015; Joseph Farrokh and Mahmoud Elhassan – USA v. Mahmoud Amin Mohamed Elhassan, Government's Sentencing Memorandum.

[305] For example: Akhror Saidakhmetov and Abdurasul Juraboev, USA v. Abdurasul Hasanovich Juraboev, Defendant's Sentencing Memorandum, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York, 2017.

> networks...[However] scholars cannot ignore the cases that appear to go against the grain, and may have to re-assess this position if instances of so-called online "self-radicalisation" increase. (Meleagrou-Hitchens and Kaderbhai 2017, pp.29–32)

These perspectives therefore raise the question of whether these five potential cases of an online only trajectory represent a growing trend or are merely the exceptions that prove the rule. Given they are so few in number compared to those that acted in both domains, it is difficult to make the case that – even in a time of greater cyber-dependence – there is a development towards online only trajectories.

6.4.3 First Steps

While it is important to establish whether actors used the Internet exclusively from their entry point into the radical milieu to their eventual activity, it is admittedly a high evidentiary bar, particularly given the weight of evidence in previous literature that suggests actors tend to use both domains. While coding the case studies line-by-line descriptively to establish whether there were online only trajectories, the data show that the Internet accounted for the first steps into the radical milieu for several actors. The majority then went on to act offline in different ways, but the filings and reporting explicitly state that the Internet was the entry point for them. Interestingly, descriptive coding highlighted several different reasons and methods for actors turning to the Internet to seek radical content. Upon constant comparison, these are selectively coded into themes which relate to how actors came to enter the radical online milieu.

Spiritual Fulfilment

Several actors turned to the Internet for a more radical interpretation of Islam because they felt they were not being fulfilled spiritually. As detailed above, Hoda Muthana, sought a more fundamental religious experience than her family could provide. Although they were deeply conservative, Muthana told a reporter that she sought a more radical interpretation of Islam, and her father's graduation gift of a cellphone provided a gateway to the radical YouTube lectures and jihadist Twitter that gave her that opportunity.[306] Ali Shukri Amin, who operated the influential @AmreekiWitness Twitter account and facilitated the travel of Reza Niknejad, told a forensic psychologist that he, too, sought a more intellectual religious experience than the ceremonial Islam that was practiced by his parents. He then researched Islam online, leading him to IS supporters, who made him feel intellectually valued.[307] For others, it was a frustration that went beyond family.

Similarly, Keonna Thomas' defence counsel claimed that she began to use the Internet when she felt that her local Muslim community was not giving her the religious structure

[306] Ellie Hall, Gone Girl: An Interview with An American in ISIS.
[307] Yasmeen Abutaleb and Kristina Cooke, A teen's turn to radicalism and the US safety net that failed to stop it, *Reuters*, June 6, 2016. Available at: https://www.reuters.com/investigates/special-report/usa-extremists-teen/.

she desired, which led to her receiving spiritual instruction from IS supporters.[308] A college friend of Warren Clark, who successfully travelled to Syria in 2015, noted that he converted to Islam in 2004, but as he became more devout, turned to the Internet, which in turn led him to radical sites and violent anti-American YouTube videos, which he would watch until the early hours of the morning.[309]

One Online Community to Another

Other actors were already in online communities which may have led them towards engaging with the radical online milieu. As described above, Safya Roe Yassin was an active member in several online conspiracy theory communities, including anti-vaccine, "chemtrails", and anti-GMO movements. Given the anti-government parallels between conspiracy theories and extremist movements, it is possible that Yassin transitioned sideways.[310] The same can be said of Christopher Lee Cornell, who sought to conduct an attack on the US Capitol during the State of the Union in 2015, who also regularly posted anti-government conspiracy theories online, for example, suggesting that the Ferguson, MO riots were part of a plot to install a "Jewish world order".[311] Cornell had few friends and recently converted to Islam and it is suggested by Abrams that 'the radical Islam he discovered online might have resonated' with such a personality.[312]

Heather Coffman, too, was someone without a significant social circle, and her defence counsel claimed she developed a strong passion for video games and social media, which became her whole social life. The defendant's sentencing memorandum suggests that through people she met in this domain, she became interested in IS and enjoyed making provocative posts on Facebook.[313] These cases suggest that, rather than the Internet being an entry point to the online radical milieu exclusively from the offline domain, some actors can transition sideways from other communities.

University

Several other actors found their way to radical content via new experiences while at university. Munther Omar Saleh was part of a plot to construct and detonate a pressure cooker bomb in New York, NY and was also part of the network of young men that sought to travel from the New York/New Jersey area. His entry point to radical content came as a college student at which time he became interested in politics. He noted that pictures of injured and orphaned children motivated him to become an activist: 'I saw the civil war

[308] USA v. Keonna Thomas, Defendant's Sentencing Memorandum.
[309] Tracy Connor, Texas Convert Warren Clark Sent ISIS His Resume, Report Says, *NBC News*, February 6, 2018. Available at: https://www.nbcnews.com/storyline/isis-terror/texas-convert-warren-clark-sent-isis-his-resume-report-says-n845151.
[310] Katie Zavadski, The American Anti-Vaccine Mom Turned ISIS Superstar.
[311] USA v. Christopher Lee Cornell, Government's Sentencing Memorandum, Case: 1:15-cr-00012-SSB, United States District Court for the Southern District of Ohio, Western Division, 2016.
[312] Dan Horn, The Terrorist Recruiter in Your Living Room, *Cincinnati*, January 18, 2015. Available at: https://eu.cincinnati.com/story/news/2015/01/17/terrorist-recruiter-living-room/21918469/.
[313] USA v. Heather Coffman. Defendant's Sentencing Memorandum.

in Syria and I was moved… I felt a connection to the people and was bothered by their suffering.'[314] Although his online messages began supporting a peaceful solution, the filings note that after months of researching the conflict online led Saleh to IS propaganda, which credibly made the case of defeating Assad, as well as promising nationhood and citizenship for him.[315] Importantly, the Government prosecutors posit that Saleh was the driving force in recruiting the other members of his network, suggesting that this entry point predates an offline network.[316]

University was also where Mohimanual Bhuiya was motivated to seek further information about Muslim conflicts. Bhuiya, who successfully travelled to and returned from the caliphate, conducted a television interview upon his return to the US. In it he described his emotional turning point at Columbia University in which he took a course called "Muslims in Diaspora", in which he watched the 2004 film "Submission" by Theo van Gough and Ayaan Hirsi Ali which depicts a women in a burqa with passages from the Koran written over her nude body. Bhuiya described the experience as "really humiliating", which led him to turn to the Internet for answers.[317] This then led to him spending "hours a day" online over the subsequent months, which eventually led to him travelling to Syria.[318]

Interest in Middle East Conflicts

As with Saleh, mentioned above, other actors found their way to radical Islamist content online via following conflicts in the Middle East. Donald Ray Morgan travelled to Lebanon in January 2014, before eventually attempting to enter Syria to join IS, but was stopped en route in Turkey and sent back.[319] In a television interview, Morgan gave a detailed explanation of his life and upbringing, saying that he was first exposed to Islam in university, but did not convert until a number of years later after his divorce in 2007.[320] However, his turn towards radical Islamism came in about 2012, a time in which he was spending hours per day following the conflicts in the Middle East and got "sucked in" and

[314] USA v. Munther Omar Saleh, Defendant's Sentencing Memorandum, p.9.
[315] USA v. Munther Omar Saleh, Defendant's Sentencing Memorandum.
[316] USA v. Munther Omar Saleh, Government's Response to Defendant's Sentencing Memorandum, Case 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018.
[317] Richard Engel, Ben Plesser and Tracy Connor, American ISIS Defector: 'I've Let My Nation Down', May 22, 2016. Available at: https://www.nbcnews.com/storyline/isis-uncovered/american-isis-defector-i-ve-let-my-nation-down-n578216.
[318] Richard Engel, Ben Plesser and Tracy Connor, American ISIS Defector: 'I've Let My Nation Down'.
[319] USA v. Donald Ray Morgan, Factual Basis, Case 1:14-cr-414-1, United States District Court for the Middle District of North Carolina, 2014.
[320] NBC News, EXCLUSIVE: American Extremist Reveals His Quest to Join ISIS, September 3, 2014. Available at: https://www.nbcnews.com/storyline/isis-terror/exclusive-american-extremist-reveals-his-quest-join-isis-n194796.

began posting statements supportive of IS on social media,[321] including statements quoting and giving homage to figures such as bin Laden and Awlaki.[322]

Samy el-Goarany, who allegedly travelled to Syria in January 2015, straddles the themes of following Middle East conflicts and already being online. El-Goarany – now deceased – had a prolific Tumblr account in which he posted about social justice, from critiques of US interventions to racism to anti-capitalist sentiments, as well as lighter themes such as music and travel.[323] He was of Egyptian heritage and kept up to date with the ongoing civil war in his father's home country. His friends noted that it was around this time that his postings became more radical in nature, and he even tweeted that the Egyptian Government's massacre of Muslim Brotherhood supporters in 2013 was a key motivator for his travel.[324] Importantly, it was via this entry point into the online radical milieu that he met Ahmed Mohammed el Gammal online in October 2014. El Gammal, who resided in Arizona but travelled to New York to meet el-Goarany, would be instrumental in facilitating el-Goarany's travel to Syria, providing him with a contact in IS and a reference.[325]

Fertile Ground

Rather than a location or interest of an entry point, the filings and reporting often suggest that actors' first steps into jihadism were due to factors such as social isolation, trauma, and mental health problems, for which the Internet provided an outlet which could likely not be replicated by offline socialisation. Harlem Suarez, who planned an IED attack in West Keys, FL began searching for radical material online in April 2014.[326] Reporting suggests that Suarez was unstable and childlike and would obsessively adopt new personas such as of a gangster, powerboat racer, and drug dealer, making 'the web… a fertile ground for emotionally immature young men like Suarez to explore all kinds of fanatical ideas.'[327] It was online that Suarez would meet an FBI undercover agent, with whom he planned his plot.[328]

Justin Nojan Sullivan, who plotted attacks in North Carolina and Virginia virtually with Junaid Hussain, told an undercover agent that 'I liked IS from the beginning then I started

[321] Richard Engel, How a North Carolina Native Ended Up on a Quest to Join ISIS, *NBC News*, September 3, 2014. Available at: https://highered.nbclearn.com/portal/site/HigherEd/flatview?cuecard=71348.
[322] USA v. Donald Ray Morgan, Factual Basis.
[323] Katie Zavadski, Mom and Dad Hid a Terrible ISIS Secret.
[324] Katie Zavadski, Mom and Dad Hid a Terrible ISIS Secret.
[325] USA v. Ahmed Mohammed el Gammal, Criminal Complaint, Case 1:15-cr-00588-ER, United States District Court for the Southern District of New York, 2015.
[326] Jessica Lipscomb, How Harlem Suarez Went From Cuban Immigrant to Wannabe ISIS Jihadi, *Miami New Times*, September 3, 2017. Available at: https://www.miaminewtimes.com/news/harlem-suarez-goes-from-cuban-immigrant-to-wannabe-isis-jihadi-9643881.
[327] Jessica Lipscomb, How Harlem Suarez Went From Cuban Immigrant to Wannabe ISIS Jihadi.
[328] USA v. Harlem Suarez, Criminal Complaint, Case 0:15-mj-05016-LSS, United States District Court for the Southern District of Florida, 2015.

thinking about death and stuff so I became Muslim.' [329] Sullivan's neighbours told reporters that he rarely left the house, and he was also unstable, murdering his next door neighbour and soliciting a contract for the killing of his parents.[330] His defence counsel said that he was depressed and suicidal and had been expelled from school, with a doctor diagnosing him with pre-schizophrenia.[331] In the words of Government prosecutors, Shivam Patel, 'began his embrace of ISIS while located in the safety of his parents' home in Virginia,'[332] also focusing on his troubled childhood and mental instability, including suicide attempts, attempting to harm a therapist while in hospital, and having multiple episodes of psychosis.[333]

The core concept which links these factors together is that the Internet can provide a diverse range of affordances which can enable ideological learning. In these cases, individuals were taken up to a certain point but felt that they needed to develop further, for which the Internet provided an outlet. For some it was a frustration with their existing spiritual existence, while for others it was a new conspiracy to help make sense of the world. For many it was an extension of learning within a formalised setting such as university, or an outlet to continue learning about conflict. Finally, it acted as an entry point for individuals that may have predispositions which could be exacerbated by such learning. Important here is the lack of regulation of ideas on social media compared to their offline counterparts – Bouhana (2019) notes that regulation has been outsourced from government to tech companies in recent years, which may promote the emergence of extremism-enabling moral ecologies. Where individuals may have been under the guidance of moderate trained professionals in the offline domain at a mosque, university, or receiving healthcare, the unstructured dialogue of social media and easy access to extreme propaganda could mean that this "jumping off" point created a dynamic which exacerbated these individuals' radicalisation.

Despite sharing the Internet as an entry point into the radical milieu, this section demonstrates the heterogeneity of terrorist pathways. There are a range of diverse factors which lead actors to turn to the Internet. This point is made by Holt et al. (2016), who argue that terrorists' heterogeneous pathways result in a lack of common points of entry to the movement, however:

> The Internet may serve a leveling function that brings all individuals into a similar point of entry. The Internet as a source of ideological messaging is on 24 hours a

[329] USA v. Justin Nojan Sullivan, Factual Basis, Case No. 1:16-cr-05- MR-DLH, United States District Court for the Western District of North Carolina, 2016, p.9.
[330] Michael Gordon, First American ISIS Convert in Custody, Justin Sullivan, to Face the Death Penalty, *Charlotte Observer*, March 18, 2016. Available at: https://www.charlotteobserver.com/news/local/crime/inside-courts-blog/article66952427.html.
[331] Michael Gordon, 'I Am Not a Bad Person,' ISIS Conspirator Says in Admitting he Murdered Elderly Neighbor, *Charlotte Observer*, July 17, 2017 Available at: https://www.charlotteobserver.com/news/local/article161716598.html.
[332] USA v. Shivam Patel, Government's Sentencing Memorandum, Case 2:17-cr-00120-MSD-DEM, United States District Court for the Eastern District of Virginia, 2018, p.15.
[333] USA v. Shivam Patel, Government's Sentencing Memorandum.

> day, providing relatively equal access to radical messages and networks where individuals may gain entrance to a group. (Holt et al. 2016, p.7)

In other words, some actors may turn to the Internet because it is the only place they can seek a radical interpretation of religion, while some may be incapable of forging social connections, but what they can find is the same: a vast amount of ideological content, peer-to-peer communications, and instructional material, among other things.

Other scholars have suggested that the Internet may act as an important entry point, particularly for seeking information. Gendron argues that for individuals that may be experiencing a crisis of identity or a sense of injustice, the 'information gathering process, which is a critical first step along the path to radicalization, is facilitated by the Internet' (Gendron 2017, p.51). Similarly, Silber and Bhatt note that in the first step of their conceptual model, the 'Internet provides the wandering mind of the conflicted young Muslim or potential convert with direct access to unfiltered radical and extremist ideology' (Silber and Bhatt 2007, p.8). These arguments seem to ring true with many of the individuals that took their first steps on the Internet; many were seeking information on different, yet related, topics such as religious doctrine or Middle East conflicts and found IS supporters or propaganda.

However, it cannot be ignored that these cases represent a relatively minor proportion of the sample as a whole. While not every case gives an indication of how the actor first became involved in the movement, many come from offline friendship networks,[334] prison,[335] family members,[336] romantic partners,[337] or via conflict zones.[338] In total, positive evidence was found to suggest that 17 actors made their first steps via the Internet – only around 8% of the sample in total. On the other hand, accurately assessing how many made their first steps offline is far more difficult because positive evidence is often not given. For example, there is little doubt that the recruitment network in

---

[334] For example: Samuel Topaz - Benjamin Mueller, New Jersey Man Pleads Guilty to Pledging to Join ISIS, *New York Times*, September 9, 2015 Available at: https://www.nytimes.com/2015/09/10/nyregion/new-jersey-man-pleads-guilty-to-pledging-to-join-isis.html. Nicholas Young – USA v. Nicholas Young, Application for Search Warrant. Fareed Mumuni - Mira Wassef, Facing 100-year sentence, Staten Islander Details his 'misguided' Transformation from Kind Child to ISIS Backer, *SI Live*, 25 April 2018. Available at: https://www.silive.com/news/2018/04/staten_island_terrorist_faces.html.

[335] For example: Casey Spain – USA v. Casey Charles Spain, Defendant's Sentencing Position, Case 3:17-cr-00123-JAG, United States District Court for the Eastern District of Virginia, 2018. Clark Calloway – USA v. Clark Calloway, Criminal Complaint, Case 1:17-mj-00287-GMH, United States District Court for the District of Columbia, 2017. Leon Nathan Davis II - Associated Press, 'I am an American': Man who was 'ready for jihad' before attempting to join ISIL sobs as he's given 15 years in prison, *National Post*, July 28, 2015. Available at: http://nationalpost.com/news/world/i-am-an-american-man-who-was-ready-for-jihad-before-attempting-to-join-isil-sobs-as-hes-given-15-years-prison.

[336] For example: Guled Ali Omar – USA v. Mohamed Abdihamid Farah et al, Criminal Complaint. Rasel Raihan - Engel, Plesser and Connor, An American ISIS Cell: The Story of 3 U.S. Recruits.

[337] For example: Muhammad Dakhlalla – USA v. Muhammad Oda Dakhlalla, Factual Basis. Zakia Nasrin – Meleagrou-Hitchens et al. The Travelers. Ariel Bradley – Ellie Hall, How One Young Woman Went From Fundamentalist Christian to ISIS Bride.

[338] For example: Pazara and the Hodzics – Hughes and Clifford, First He Became an American—Then He Joined ISIS.

Minnesota began with offline peer-to-peer relationships, which the filings and reporting discuss at length, but in most cases do not posit a "first contact" instance in the same way as the cases of online "first steps" are outlined above.[339] Despite this, at least 40 cases were deemed to have enough evidence to identify the entry point as offline, although given the skewed reporting; it is far more likely that offline cases are undercounted than online ones.

This prevalence towards an offline entry point as the norm is supported within the literature. Hussain and Saltman (2014) argue that the vast majority of individuals come into contact with extremist ideology through offline socialisation prior to being further indoctrinated online; those that visit 'extremist websites and consume the content enthusiastically are likely to have been heading in that direction, and the websites in question are merely aiding an existing journey' (Hussain and Saltman 2014, p.61). Similarly, in interview-based research with returning foreign fighters, El-Said and Barrett (2017) consider the role of the Internet, finding that there was a range of views in how important it was to their recruitment. However, they found that:

> Would-be [foreign fighters] appeared to turn to the Internet to confirm and strengthen ideas, perceptions and narratives that they had already developed or were beginning to develop. The Internet then played a key role in reinforcing a decision that had in part been taken already. This seemed particularly true when the process was also associated with friendship or network ties. (El-Said and Barrett 2017, p.39)

The findings illustrated above support both Hussain and Saltman and El-Said and Barrett; it only appears to be a minority of actors for which the Internet was the entry point to radical jihadism, particularly when compared to offline connections. As Chapter 5 finds, almost all actors ended up using the Internet either as part of a network of co-ideologues or to learn or plan their event, but there remains little evidence that many used it as an entry point.

6.4.4 Synthesis

While Chapter 5 made inferences about the use of the Internet for the sample as a whole, this section was intended to look specifically at the dynamics for individuals engaged heavily online. The first part sought individuals who were candidates for an "online only" radicalisation, finding that there were only five potential cases in which this is the case. Analysing and comparing these cases, four of the five demonstrated a high degree of social isolation, suggesting that this could be a stressor which pushed them towards the radical online milieu, or alternatively, the converse could be true: engaging online could have caused them to isolate themselves from their existing social circles. When sampling

[339] For example: USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint; Mike Eckel and Harun Maruf, "Why He Chose to Leave This Good Land?", *Voice of America*, [No Date]. Available at: https://projects.voanews.com/isis-recruit-somali-americans/; USA v. Mohamed Abdihamid Farah et al, Criminal Complaint.

the wider cohort, this theme appears in several other cases too. The second part analysed those that used the Internet as an entry point to the radical milieu, finding a range of different "jumping off" points, such as a need for spiritual fulfilment, moving sideways from other online communities, continuation of university learning, interests in Middle East conflicts, as well as individuals with predispositions that could be exacerbated by extremist narratives. The core concept which links these factors is the affordances that the Internet offers, providing the individuals with far less regulated or structured learning opportunities, which includes easier access to radical content.

These two dynamics are related; the latter can be seen as a wider explanation for the former. One can consider social isolation as a problem which can be remedied by specific affordances that the Internet provides. If individuals are unwilling or unable to maintain face-to-face social contact, then the Internet affords them an ability to drastically widen their pool of potential co-ideologues that can offer social gratifications. Von Behr et al. (2013) note it is widely available and enabling connection with like-minded individuals from across the world, or as Koehler (2014) observes that it is a cheap and efficient method of communication which is particularly useful for "social purposes." In essence, an online community can be sought out to supplement the lack of an offline community in these instances.

However, there are marked differences between the types of communities that can be found on social media platforms compared to face-to-face communication, which may in turn affect radicalisation dynamics. Saifudeen (2014) notes that online activity is analogous to a buyers' market in which individuals can choose communities and interactions that appeal most to them. In the examples given above, some actors may choose radical communities which offer a more theological or spiritual bent, while others engage with co-ideologues that are interested in Western foreign policy. Engaging in an offline network is unlikely to offer the actor this degree of flexibility to move between groups to find one that suits their needs. Neo (2016) offers a related point, suggesting that having found ideas that intrigue the individual, the Internet offers a greater ability to play with ideas with relatively little consequence. The online environment in which these terrorists operated in the mid-2010s and the protection of the First Amendment, means that the expression of ideology to part of an ongoing socialisation process had little in the way of immediate consequences.[340] Neo argues that this may exacerbate radicalisation because individuals can seek out alternative belief systems in accordance with their specific triggers, needs and vulnerabilities, perceived injustice, or need for adventure. Ultimately, it gives the individual far more choice than they would have had if they operated solely in the offline domain.

A proponent of the Onlife thesis would suggest that this buyers' market is a hallmark of the contemporary information environment. At first glance, it may appear that a move

[340] Of course, in many cases the consequence was the FBI opening an investigation, possibly leading to arrest or imprisonment. However, the crime was not the expression of ideas, but when the individual eventually decided to act upon them.

towards greater access of information would increase heterogenous viewpoints and provide resilience against an echo chamber effect, which is often theorised to play a role in radicalisation (For example, see: Ducol et al. 2016; Neo 2016; Neumann 2013a; Sageman 2008). However, Broadbent and Lobet-Maris (2015) argue that the buyers' market represents a significant change from previous generations in which information was scarce because it was difficult to access and disseminate. In the hyperconnected world there is an abundance of information, but little capacity to digest it. They argue that this has led social media companies designing their platforms to retain attention as long as possible according to their interests which they argue results in volatile identities with little empathy. Similarly, Thorseth (2015b) argues that people lack the capacity to absorb views that diverge from their own narrow interests in spite of the wide information available to them. This point is made by Ducol and colleagues (2016) too, who suggest that platforms are specifically designed to foster homophily by encouraging users to "follow" those with similar views, which may help to foster deviant communities.

Taken together, this section suggests that the affordances that the Internet offer can act as a radicalisation dynamic by fulfilling needs that cannot be met offline, and in doing so, offers an almost limitless possibility of gratifications in a fundamentally different environment. In this sense, von Behr and colleagues put the point well when they summarise their research in this way:

> The internet has to be seen as a mode, rather than a unitary method, of radicalisation (the internet can play an important role in facilitating the radicalisation process; however, it cannot drive it on its own). Instead, the internet appears to enhance the process. (Von Behr et al. p.33)

The Internet can offer new opportunities for would-be terrorists, but it is ultimately just a tool for them to explore and shape their own radicalisation. Even if individuals do act entirely online, or first enter the radical milieu, any online dynamics will intersect with existing dispositions, stressors, and vulnerabilities, or as Durodie and Ng put it: 'No individual approaches the Internet in isolation. They come to it already bearing a vast number of ideas, assumptions and emotions' (Durodie and Ng 2008, p.2).

It is worth reiterating that the individuals identified at the heavy-usage end of the spectrum are relatively uncommon within this sample. Only five cases were identified as possible online-only cases and seventeen instances in which the Internet acted as the entry point to the radical milieu, suggesting that each are still a relatively rare occurrence. It is also instructive to note that the trend of online only radicalisation does not seem to be growing, even in a time of greater cyber-dependence, as has been suggested by some scholars (Institute for Strategic Dialogue 2011; Meleagrou-Hitchens and Kaderbhai 2017), and it appears that most individuals are already engaging with radical ideologies prior to turning to the Internet (El-Said and Barrett 2017; Hussain and Saltman 2014). This supports the quantitative findings of Chapter 5, and previous research which found

that the sample tended to act in both domains (Gill et al. 2017; Reynolds and Hafez 2017; Von Behr 2013).

Grounded Theory

3. *The Internet can act as tool for individuals to fulfil their needs that cannot be met offline in a flexible and constraint-free manner.*

6.5 Conclusion

This chapter has used a grounded theory-inspired methodology to inductively assess the online behaviours of 201 IS actors in the US, discovering three substantive radicalisation theories from the data. The first section analysed the radical content that they collected, consumed, and created, finding that engagement with propaganda is best seen as an ongoing socialisation process between actors in the online radical milieu in which actors can construct radical identities. The second section looked specifically at female actors' online activity, finding that it is possible to use the Internet as a space to perform a less restrictive gender identity than offline Salafi networks would permit. Finally, the third section examined individuals that used the Internet heavily as part of their trajectory, demonstrating that the Internet can act as a tool for individuals to fulfil their needs in an environment with more flexibility and fewer constraints.

While these radicalisation dynamics should stand alone for exploration in future research, it is worth noting that there are some important commonalities between them which elucidate the contemporary information environment. Firstly, this chapter demonstrates that radicalisation trajectories are invariably social; individuals did not merely turn to the Internet to passively consume information and "self-radicalise". Instead, each of the sections shows that terrorists engaged in social processes by seeking a wider network to continue their ideological learning and, importantly, perform it to their new audience. Secondly, and relatedly, each of the sections shows that the online radical milieu is a malleable space. By using online platforms, actors can pick and choose the type of propaganda or social contacts that suits their specific needs. This can be seen in the high prevalence of AQ content – a rival to IS – to the use of memes to the various online entry points. It allowed the women in the second section to create the personality that suited their needs rather than being bound to traditional gender roles.

Finally, the findings of this chapter support much of the Onlife thesis. Many of the ways in which individuals acted blurred the distinction between the online and offline domains, such as consuming online propaganda in offline groups; having face-to-face discussions about the content they had previously watched online; or taking risky photos or videos to upload to social media. This type of activity suggests that within the contemporary information environment, it makes little sense to have a hard dichotomy between the two domains. At first glance, this may seem at odds with the latter two sections of this chapter, which suggest that there *is* a meaningful difference between acting online and offline. However, as will be elucidated in the following chapter, the most

ontologically sound position is to consider an individual's full information environment, consisting of a range of online *and* offline interactions, which may include platforms or dialogues that offer different affordances, but can be assessed within a holistic theory of radicalisation.

Chapter 7: Discussion

7.1 Introduction

This thesis has offered three important original contributions to the academic literature, which will be elucidated in this chapter. Firstly, it has offered an empirical insight into the demand-side of research into terrorists' use of the Internet using a mixed methods approach. The findings suggest that the Internet is an important aspect of contemporary pathways towards terrorism, but ultimately, that demarcating terrorist behaviour into the online and offline domains is a false dichotomy.

Secondly, it has offered theoretical contributions to the online radicalisation debate at different levels of abstraction, including radicalisation dynamics which are grounded in the data; an ontological challenge based on the false dichotomy described above; and, given this, this chapter will then propose that a more holistic radicalisation theory is better suited for understanding the role of the Internet in contemporary trajectories, as well as giving a fuller explanation of how individuals' environments affect their norm-based motivations.

Thirdly, the findings offer an important insight into policy debate; the radical jihadist ecosystem is fragile and it is possible that the removal of terrorist content and suspension of users from online platforms is hampering law enforcement efforts to detect, track, and build cases against terrorist actors. However, this goes precisely against the current direction of travel – governments are seeking to compel platforms to remove as much content as possible. This could have unintended consequences that make terrorists migrate to more secure platforms that do not comply with subpoena or government takedown requests.

After discussing these contributions, this chapter highlights several limitations of this research, such as the focus on a single group, a lack of comparable base rates, the reliance on secondary sources, and the potential for subjective differences in coding. The chapter finishes by offering a range of avenues to continue this project in future research, including: testing the theoretical propositions that were established in Chapter 6; compiling terrorists' behaviours in sequence analyses; comparing the affordances of social media platforms; as well as looking to see how changes in the future may affect the findings presented above.

7.2 Empirical Contribution: The Role of the Internet in Contemporary Terrorist Pathways

First and foremost, this thesis has provided an empirical contribution to a field with a dearth of data-driven research. This has been a longstanding problem in the field, identified at least as far back as Von Behr et al. (2013), who note that the lack of available

datasets to study online radicalisation has led scholarship to focus on the "supply" of content – i.e. analysis of content – at the expense of studying terrorist pathways. This point is also made by Gill and colleagues (2017), who note that data-driven studies on online radicalisation have been rare, pointing to their literature search of 200 abstracts, of which only 6.5% used data of any kind, and 2% used primary data. Conway (2016a) notes that the field has sizable knowledge gaps because basic descriptive research is missing, which is a precursor to more complex theory-driven research. More recently, Scrivens, Conway, and Gill (2020) note that despite a recent surge in research, there remain few empirically-grounded analyses on the topic.

This thesis has contributed to the field by providing such an empirically analysis to better understand the role of the Internet in radicalisation pathways. This has been done using an approach that draws from a range of methods. Chapter 5 utilises a mostly deductive and quantitative approach which derived four research questions from the academic literature and replicated several coding variables that were utilised in previous studies for the basis of comparing this research population against previous ones. In Chapter 6, the data were subject to an inductive and qualitative analysis, deriving findings from the data which were synthesised into radicalisation dynamics. These contrasting approaches were chosen to complement each other and build on the other's weaknesses, as advocated for by Greene (2007) and Bryman (2006). The first provided generalised findings for the whole cohort of 201 terrorists but is limited to a mostly binary coding system of 1s and 0s, while the second took a deeper dive at individual cases to identify more complex dynamics. In essence, it has tackled the same dataset using two very different approaches.

The empirical findings provide support to the existing view that the Internet is ubiquitous in contemporary cases of terrorism (Bastug et al. 2018; Jensen, James et al. 2018; Gill et al. 2017; Von Behr et al. 2013). Chapter 5's RQ1 sought to establish the prevalence of the Internet, and in what ways it is used. The quantitative findings showed that over 90% of actors used the Internet as part of their antecedent behaviours. Moreover, they displayed a wide range of different online behaviours, including networking activities such as disseminating propaganda, supporting others, and recruiting others, as well as learning or planning behaviours such as preparing for plots, accessing propaganda, or overcoming hurdles. Terrorists also used a wide selection of different social media platforms, including mainstream ones, suggesting that there is a wide ecology which sustained the radical online milieu (Conway et al. 2017; Fisher, Prucha, and Winterbotham 2019). The use of the Internet is greater within this sample than in many previous studies. The most logical explanation is that the data are from a more recent timeframe, one in which the Internet has become ubiquitous. However, differences in the richness of data, location, and coding are also possible explanations.

The findings of the qualitative analysis in Chapter 6 support the notion that the Internet is important in contemporary cases of terrorism. Actors in the sample collected and consumed a wide array of different types of content, almost exclusively online. This

includes official IS propaganda, that of rival groups such as AQ, and speeches from preachers such as Anwar al-Awlaki. Actors also created and shared a large amount of low-level content themselves, including uploaded text-based posts, photographs, and memes. Similarly, when looking at how the female actors used the Internet, several "influencers" had a sizable social media presence, often boasting a large number of followers, and may be central to the online jihadist network.

Taking both chapters together, these points suggest that the Internet is prominent in pathways towards terrorism. Actors are highly engaged in the online domain; there is a cyber footprint in almost every case within this sample and, moreover, actors use the Internet for a wide array of behaviours. This is doubtless in part because of the affordances that are offered, such as instant, easy, and cheap communication that can connect actors across the world, as argued by the ISD:

> The internet has transformed the way we communicate; it has dramatically reduced the cost of communication; it has enabled unlimited access to much of the world's knowledge…it has made it easier to find people and create networks among like minded individuals, across great distances and beyond national borders…It is not surprising that terrorists and extremists have adopted it as one of the tools of their trade. (Institute for Strategic Dialogue 2011, p.1)

In the case of IS, it has enabled the spread of propaganda in audio-visual formats from the battlefields of Syria and Iraq to devices in the US (Klausen 2015; Carter et al. 2013), as well as allowing experienced terrorists to provide operational support and inspiration to inexpert audiences (Alexander and Clifford 2019; Hughes and Meleagrou-Hitchens 2017).

Given these findings, it may seem intuitive to lend support to an "online radicalisation" thesis, such as that argued by Sageman (2008a), Weimann (2012), and others (Post, McGinnis, and Moody 2014; Anti-Defamation League 2014). RQ2 analysed the relationship between the online behaviours that actors exhibited and their offline ones. Investigating RQ1 shows that almost every actor used the Internet, actors tended to operate in both domains. That is to say, those that interacted with co-ideologues online also tended to communicate with them offline, and actors that used the Internet to learn about or plan their eventual activity also did so in the physical world. This is congruous with the findings of Gill and others and von Behr et al., whose research suggests that while the use of the Internet is high, most terrorists act in both the online and offline domains (Gill et al. 2017; Gill and Corner 2015; von Behr et al. 2013). It also highlights the importance of offline networks of co-ideologues, supporting previous research which has posited this as a key factor in radicalisation and recruitment (Meleagrou-Hitchens, Hughes and Clifford 2018; Reynolds & Hafez 2017; Elsayed & Barrett 2017; UN-CTED 2015; Soufan Group 2015).

The spread of antecedent behaviours across both domains was also a recurring theme in Chapter 6. Even though many actors in the sample used the Internet to procure and

consume propaganda, this was often done in relation to face-to-face peers. Actors held "viewing parties" in which they watched Anwar al-Awlaki videos with their friends, or they would watch content online and then discuss with co-ideologues face-to-face afterwards. These findings support the research of Baugut and Neumann (2019), who argue that the consumption of propaganda is not easily demarcated into online and offline; rather the two domains are intertwined and feed into each other. Similarly, Chapter 6 also focused specifically on those that used the Internet heavily, finding that there were only five cases of potential "online only" radicalisation compared to the at least 167 actors that engaged in the offline domain. This supports much of the wider literature which plays down the existence of "online only" trajectories (Meleagrou-Hitchens and Kaderbhai 2017; von Behr et al. 2013; Reynolds and Hafez 2017). Moreover, there were only seventeen instances where the actor's entry into the radical milieu was via the Internet, supporting previous research into terrorists' trajectories, suggesting that most actors are already on the pathway before turning to the Internet (Hussain and Saltman 2014; El-Said and Barrett 2017). For the most part, actors in this cohort came online via existing networks and kept in contact with them.

Having established that the online domain is not replacing the offline as the primary venue for radicalisation, RQ3 questioned whether terrorists that use the Internet displayed markedly different experiences than those that did not. The findings here were more mixed; some types of plotters were more likely to use the Internet to communicate with a network, like financiers or facilitators, while others were less likely, such as attackers (although attackers that plotted attacks with an IED were more likely to do so). However, there were a range of null findings that are instructive. Lone actors were *not* more likely to engage in either ideological or preparatory learning via the Internet, nor were those that plotted more sophisticated attacks. These findings differ from previous research conducted by Gill et al. (2017), who found significant correlates for both. On the other hand, the lack of significant correlates between age and Internet activity supports previous research by Gill and Corner (2015).

The notion of a different experience is also explored in Chapter 6, but in different ways. While the quantitative results of RQ3 found that female actors did not use the Internet more than male ones in general, a deeper, qualitative dive into the 20 female actors found there were stark differences within the sub-group. Some women were highly networked online "influencers" that had great reach, others barely had any online footprint at all, while others took more of a balanced approach. Similarly, a focus on the actors that used the Internet heavily found that, even though the number was small, some individuals were potential candidates for "online-only" radicalisation. Both sets of findings demonstrate that terrorist populations tend to be heterogenous (Horgan et al. 2016; Bakker 2006; Sageman 2004) and their radicalisation pathways include a range of diverse experiences (Helfstein 2012; Borum 2011b; King and Taylor 2011; McCauley and Moskalenko 2008; Horgan 2008; Borum 2003). While the quantitative analysis demonstrates that *in general* there are minimal differences in experiences between those

that use the Internet and those that do not, the qualitative chapter took a more nuanced approach to analysis to highlight instances in which there are differences.

RQ2, RQ3 and the findings of Chapter 6 demonstrate why it is vital to assess the role of the Internet *in relation* to offline behaviours. If one were to take the descriptive findings of RQ1 and merely assess online radicalisation on the basis of descriptive statistics and the use of the Internet then it would dramatically overcount the phenomenon. This persists within the existing literature – Bastug et al. (2018) for example, collect wider data on background variables and offline networks, but seemingly make decisions as to whether actors were radicalised online on the basis of social media usage alone. As both Benson (2014) and Neumann (2013a) note, it is unsurprising that terrorists use the Internet to network, advocate, and consume content – we all do. Whichever definition of "online radicalisation" is used – whether it is online-only, mostly online, or some kind of causative effect – it requires a comparison of the Internet compared to other factors, which is the approach taken in this thesis.

7.3 Theoretical Contributions

Building on the empirical findings, this thesis offers a significant theoretical contribution for understanding online radicalisation. This is done at three levels of abstraction, which will be discussed below. The first is the substantive radicalisation dynamics that are derived from the grounded theory analysis in Chapter 6. Rather than cause and effect theories, these dynamics may exacerbate an individuals' radicalisation but should be seen as neither necessary nor sufficient. The best frame for understanding these within the literature is the "pyramid model" of radicalisation by McCauley and Moskalenko (2008), who outline 12 mechanisms, which they do not claim is exhaustive, nor do they posit a single underlying theory to unite them. The second theoretical contribution builds the empirical findings into the ontological view proposed by Floridi and other "Onlife" scholars; it does not make sense to think of the online and offline domains as separate but instead as a single dynamic information environment. Finally, given this ontological position, this chapter will build on a holistic view of radicalisation which incorporates actors' whole information environment without having to rely on demarcations that are difficult to defend.

7.3.1 Grounded Theory: Radicalisation Dynamics

The first radicalisation dynamic is derived from a qualitative analysis of actors' consumption and creation of radical content. While existing radicalisation theories have often focused on content as directly motivating and radicalising individuals (Weimann and Von Knop 2008; Torok 2013; Saifudeen 2014; Neo 2016), this research posits engaging with propaganda as part of an ongoing socialisation process. Rather than passive consumers for whom radicalisation is a thing that happens *to* them, individuals actively engaged with co-ideologues, seeking out discussions and new opportunities to engage. This is in line with existing theories, which point to the importance of social dynamics in the radicalisation process (Webber and Kruglanski 2017; Helfstein 2012;

McCauley and Moskalenko 2008; Sageman 2004). While this does not preclude the possibility of propaganda motivating individuals to conduct acts of terror, it is better seen as "mood music" for this social process. Importantly, social media platforms such as Facebook and Twitter, play an important part in contemporary socialisation. They are built with architectures that promote staged authenticity and the ability for individuals to construct idealised versions of themselves (Gündüz 2017; Burkell et al. 2014; Uimonen 2013). In this dataset, several terrorists constructed a radical, pious, and warrior-like avatar that was intended to demonstrate to their audience that they were worthy of IS, similar to that theorised by Brachman and Levine (2011).

The concept of space is also key to the second grounded theory derived from the data. An examination of the 20 women in the sample finds that several used the Internet as a space to construct an identity that may be fundamentally different to their offline persona, which would have been limited in offline circles due to their restriction from gender mixing in the Salafi jihadist movement. Much like the previous section, women were able to use this space to carve out their own emerging identity in a freer and more social way, supporting the findings of previous research (Pearson 2016; Halverson and Way 2012; Picart 2015). For some, this meant breaking down socially mandated rules forbidding male and females talking, while others took it one step further and actually pretended to be men on some platforms. There was no single way in which women did this – the women in this sample took many roles – and many chose to eschew the Internet altogether. However, the Internet, and the specific affordances of social media platforms – such as anonymity (Neumann 2013a; Sageman 2008) and norms that differ from face-to-face conversations (Ducol et al. 2016) – offered the ability for individuals to act in an environment that gave them the freedom to choose.

The freedom that the Internet provides radicalising actors is also a core component of the third dynamic. Beginning with an investigation as to whether some individuals had "online-only" radicalisations, it was found that of the five potential candidates, several of them (as well as members of the wider cohort) displayed social isolation and used the Internet as a way of mitigating it. Moreover, an analysis of the individuals that first entered the radical milieu via the Internet shows that each did so to fulfil needs that were wanting in their face-to-face interactions. Therefore, for both groups, the Internet provides individuals the freedom to choose from a wide selection of content or contacts to fulfil them. The importance of the Internet is key here, which provides users with an almost unlimited supply of potential information that can aid ideological development or provide peer-to-peer contact (Koehler 2014; Von Behr et al. 2013). The analogy made by Saifudeen (2014) of a "buyer's market" is key here; individuals have the freedom to choose what kind of radicalisation experience suits them and play around with it on platforms with relatively few consequences (Neo 2016).

These three dynamics are interlinked; they all posit radicalisation as a social process in which individuals turn to the Internet for fulfilment, which in turn provides them with a large degree of space and freedom due to the affordances of online platforms. Although

most conceptualisations frame the process as being a personal one, as discussed above, several scholars have highlighted the importance of socialisation. Helfstein (2012) explicitly argues that the role of socialisation is important and cannot be easily separated from ideology, while McCauley and Moskalenko (2008) include only two of their twelve mechanisms as being at the individual level, with the other ten involving some other kind of group dynamic. Webber and Kruglanski's model (2017) also stresses that the needs of radicalising individuals are both personal and social. A number of theoretical contributions also highlight the importance of social interactions. Sageman's "bunch of guys" theory posits that individuals' pathways are invariably driven by feelings of kinship and brotherhood (Sageman 2004), while Wikström and Bouhana's (2017) research using situational action theory seeks to better understand the relationship between individuals and their environments. Borum (2011a) lists a number of theoretical contributions that rely on social processes which may play a role in explaining mobilisation including social movement theory, which highlights the importance of collective group identity, as well as groupthink, which posits that the need for social consensus within groups will override the goal of making the most appropriate decision.

The empirical quantitative findings of Chapter 5 also support the notion of radicalisation as a social process; almost 80% of actors engaged in direct online peer-to-peer communication and those that did also tended to do so offline. Even the subset of lone actors was just as likely to communicate with co-ideologues as their group-based counterparts, supporting the notion that lone actors are rarely alone, but instead often sought to take part in group-based activities with like-minded peers (Schuurman et al. 2017; Gill, Horgan and Deckert 2014). There is no single life-course or process that individuals take on their pathway towards terrorism, supporting previous research, like that of Corner and Gill (2019), Vidino, Marone and Entenmann (2017), and Bakker (2006), who note the lived experience of being a terrorist is a heterogeneous one with vast differences in life experiences. However, this research consistently re-affirms that the routes actors take are routinely social ones, albeit in different ways. Forging and maintaining social connections is important for the vast majority of actors within this sample. Actors do this in several different ways and the contribution of this research is to show the different mechanisms involved, specifically the interplay between the online and offline domains.

Conceptualising the process of becoming a terrorist as inherently social offers an important insight into the role of the Internet. Part of the false dichotomy between the online and offline domains that is outlined above is that oftentimes, the former is assumed to be "less social" than the latter. This has been challenged by Conway (2016a), who describes the language used in the literature of online radicalisation as privileging "real world" activity. She takes a report by the UK Home Affairs Select Committee to task, who claim that extremist material on the Internet 'will rarely be a substitute for the social process of radicalisation' (UK Home Affairs Select Committee, quoted in: Conway 2016a, p. 4). She argues that the authors of the report have misunderstood the social nature of social media:

> Today's Internet does not simply allow for the dissemination and consumption of "extremist material" in a one-way broadcast from producer to consumer, but also high levels of online social interaction around this material. (Conway 2016a, p.4)

The social interaction that Conway argues for is the new norm; it is no longer possible to demarcate "going online" from living in the "real world". This is discussed in greater detail below.

On this reading, socialisation between peers as part of pathways towards terrorism is something which occurs regardless of the level of technology available. It is, of course, important that this type of technology offers unparalleled affordances in reach, allowing for individuals to reach the battlefields of Syria instantly and cheaply via social media platforms (Klausen 2015; Carter et al. 2013). Similarly, the manner of online discourse may well be different to face-to-face communications, or site architectures such as recommender algorithms may artificially push people towards certain types of content (Reed et al. 2019). It is possible that these factors may yield crucial differences in the pathways that terrorists take towards their eventual activity. However, technologically mediated communication has always been different to face-to-face discussion. The invention of the telephone in the nineteenth century completely changed the reach and speed with which people could communicate. Furthermore, reading Irish Republican Army pamphlets from the 1970s was a fundamentally different way of engaging with radical content than attending rallies. Terrorists have frequently been early adopters of technology and the Internet is no different (Bloom et al. 2017; UN CTED 2015). Rather than framing the use of the Internet as something fundamentally new – as "online radicalisation" – it is better to view it as a continuation of the use of communications technologies which individuals use, among other things, to socialise with their peers.

7.3.2 Onlife Radicalisation?

When considering the question of online radicalisation, this thesis' empirical and theoretical contributions may appear somewhat at odds. The quantitative analysis of Chapter 5 downplayed the notion that the online domain had become the new norm for radicalisation, while the qualitative analysis of Chapter 6 highlighted many of the unique traits of the Internet, which may exacerbate radicalisation. This position can be remedied however, by understanding the ontological fragility of demarcating the online and offline domains, as argued by the "Onlife" scholars in Chapter 3. Rather than seeing the two as dichotomised, it is better to understand the two as a single information environment which contains a range of Internet-based platforms *and* face-to-face interactions which are dynamically inter-related and often inseparable.

As noted in Chapter 3, several scholars have challenged the idea that there is a meaningful difference between "online" and "offline" in the contemporary world. Floridi et al. (2015a) argue that the development of technology has led to a blurring of the distinction between reality and the virtual; new artefacts no longer operate according to human instructions but instead now record data, compute it, and feed it back into a range of

machines, which in turn creates new opportunities for adaptive and personalised environments. Jurgenson (2012) refers to thinking about the online/offline dichotomy as "digital dualism," which he believes to be fallacious. The advancement of communications technologies has continually linked the two domains to the point in which they have become inseparable. He suggests that a better frame is to understand the two as an augmented reality in which social media supplements offline lives, rather than replacing them. This position is also advanced by Rey & Boesel (2014), who challenge the naturalistic fallacy that being offline is the primordial state of being, which ignores how the two domains are interrelated. They argue that humans use social media to express personal agency as well as experiencing our online avatars or devices are part of ourselves. In their view, the online and offline worlds are co-produced, and experiences are created simultaneously and humans are embodied both by organic flesh and digital protheses.

Framing the findings of this thesis through the ontological lens of "Onlife" may offer a clearer picture in explaining contemporary radicalisation trajectories. As has been established in this research and that of others (Ducol 2015; Gill et al. 2017; Valentini, Lorusso and Stephan 2020), there is no easy online/offline dichotomy to be drawn. Instead, a whole information environment offers a more holisitic understanding – an infosphere in which hyperconnected humans interact inseparably with both silicon and carbon-based objects form an augmented reality (Floridi 2007; Jurgenson 2012). On this interpretation, one would not expect that online radicalisation would replace offline radicalisation, as Sageman (2008b) suggests; the two are not in competition because they do not exist independently of one another.

A good example of the fragility of the online/offline dichotomies is the "viewing parties" that terrorists in this sample attended, as discussed in Chapter 6. Seventy percent of actors used the Internet to procure and consume propaganda, but this was often done alongside face-to-face interactions. Several acquired Anwar al-Awlaki videos on streaming platforms and gathered as friends to watch and discuss them together. Others did not necessarily watch propaganda together, but they still discussed videos they had watched in offline settings. Viewing online propaganda has typically been seen as a key mechanism of online radicalisation (Weimann and Von Knop 2008; Neumann 201a3; Koehler 2014; Saifudeen 2014), but as these examples show, viewing online propaganda is not limited to the Internet, but instead protrudes into offline behaviours as well. These findings mirror the interview-based research of Baugut and Neumann (2019), who found that their sample of radical Islamists would watch online propaganda and then discuss it with peers or preachers in an offline setting, or conversely, offline discussions would prompt them to find online propaganda. In short, even streaming videos from social media platforms cannot be considered an online activity that exists autonomously of the offline domain.

As noted in Chapter 6, several individuals used social media to construct an idealised pious identity that portrays a readiness to fight – what Macdonald and Lorenzo-Dus

(2019) describe as the "Good Muslim." While one may be inclined to view the construction of a radical online identity as evidence of online radicalisation, this can be better explained as part of an Onlife framework. Hildebrandt (2015) notes that computational layers that mediate our perception of the world are generating an environment that simulates agency, leading to a public performance and management of reputation on social media platforms. This performance then enters a feedback loop of constant measurement and calculation (e.g. likes, shares, comments). This rewards individuals that seek to explore the idealised character of their ideology. Importantly, this is not merely an online activity, but inseparably related to offline as well. Individuals chose to take photos in physical spaces and make gestures like the taweed symbol or flying ISIS' black standard flag. The fact that it was being beamed through cyberpsace for "likes" and "shares" is only half the story, the other half is that they were choosing to engage with terrorist symbolism in offline venues that they deemed to be hostile enemy territory. Social media does provide a potential audience of willing observers where previously there may have been none, but it also teaches users to look for the perfect photo, check-in, or status update in physical spaces (Jurgenson 2012).

The quantitative results in Chapter 5 suggest that terrorists that engage online as part of their plot are less likely to be successful than those that do not. A closer inspection suggested that individuals like Heather Coffman recklessly telegraphed their ideology, which resulted in the FBI opening an investigation. This is difficult to explain from a rational actor perspective – which would question why an individual would put their stated goals at risk in an environment from which it is easy to gather intelligence. Onlife scholars have argued that the changes in technology over recent decades have dramatically altered perceptions of privacy. Thorseth (2015a) argues that like the online/offline dichotomy, public and private interactions are often discussed as if they are distinct. However, she argues that this is no longer the case; conceptions about privacy have changed and young people discuss previously sensitive matters such as politics or sexuality on public platforms with little conception of privacy. Instead, Ess (2015) argues that young people use social media to carve out a space to negotiate the identity that they want to be, regardless of concerns over privacy. In essence, the performance of carving out one's radical idealised identity and using it as part of a socialisation process may be more important to terrorists than operational security, which may help to explain why some were making such reckless decisions for the sake of profile pictures or status updates.

One must also consider how the idea of online and offline networks interact with each other. This thesis found that the vast majority of terrorists engaged in an online network, but those that did were significantly more likely to engage in an offline one too. Previous research has considered these variables as competing hypotheses for the existence of online radicalisation – i.e. if online networks are more prevalent this suggests online radicalisation, but the existence of offline networks acts as a null hypothesis (for example, see: Reynolds and Hafez 2017). However, it is important to understand how being situated in (and around) radical face-to-face networks effects propensities to engage

online. Offline proximity is an important factor in content sharing algorithms (Valentini, Lorusso and Stephan, 2020), which could mean that users are more likely to be shown content or recommended friends or followers if they come from an individual in an offline network. This again casts doubt on the ability to easily demarcate between the two domains.

7.3.3 Understanding Radicalisation Environments

If we accept the ontological claim that the online and offline world are inseparable, this raises the question of how we consider contemporary radicalisation. Clearly, the notion of "online radicalisation" as offering a distinct experience would be rendered redundant – as would "offline radicalisation." Gill and colleagues argue that rather than a fixation on the location of radicalisation – i.e. online, offline, prisons, universities, schools, places of worship – that 'we need to understand the drives, needs, and forms of behavior that led to the radicalization and attack planning and why the offender chose that environment rather than purely looking at the affordances the environment produced' (Gill et al. 2017, p. 114). Terrorists in this sample used a range of different online platforms for several different reasons and it may offer them different things – for some it provided a community when the actors were socially isolated; for some it was operational; while for others it provided ideological inspiration. Simply fixating on the broad location (i.e. online vs offline) is not only ontologically unsound, but is also unlikely to yield a greater understanding of why actors engaged in the radical milieu.

Rather than a single theory of online radicalisation, it is more fruitful to consider online interactions as part of a wider criminological theory that encompasses individual and environmental factors. Situational Action Theory (SAT) can be a useful framework for understanding radicalisation pathways in the context of Onlife. Wikström and Bouhana (2017) propose that SAT can help to explain terrorism by examining the relationship between an individual and their environment and how the criminogenic inducements affect terrorists' norm-based motivations. This interplay can help to explain why individuals perceive their actions as morally acceptable, or why they fail to adhere to personal morality when their environment incites them to break it.

The main formulations of SAT within the sphere of terrorism studies have tended to assume an ontological distinction between the online and offline domains. Bouhana (2019) demarcates two types of environment in which individuals engage: social selection such as residence and socioeconomic status and self-selection, such as political rallies or activity on the Internet. Considering an Onlife ontological interpretation, the Internet would protrude across both categories, rather than being confined to purely self-selection. For example, Bouhana notes that 'living in a particular neighbourhood or belonging to a particular social group (ethnic group, religious, professional, and so on) affects the chance of exposure to certain places and the participation in certain activities' (Bouhana 2019, p. 14). However, as already established, these factors affect an individual's online activity too; online networks are strongly related to offline ones and the locations in which they exist. As outlined in Chapter 3, Ducol (2015) also argues that

SAT can help to explain the role of the Internet in radicalisation, suggesting that there are several online and offline "life spheres" and if enough are dominated by radical sociability, then it can create a gradual cognitive monopoly which can lead individuals towards terrorism. As Figure 20 shows, Ducol demarcates between online and offline life spheres, but this is not a defensible distinction – for example, "family" or "friends" cannot be easily separated from "social media."

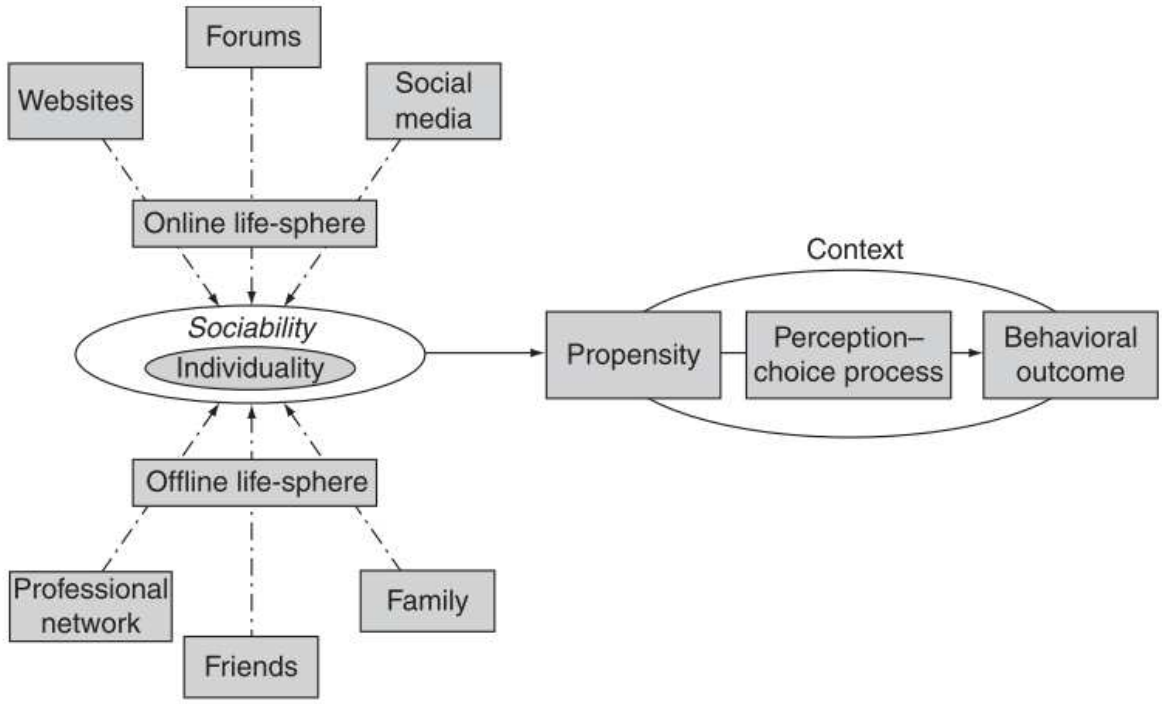


Figure 20 - Ducol's (2016) "Life Spheres" SAT Framework

This issue aside, SAT offers a better perspective to understand radicalisation trajectories – including the role of the Internet – than the online radicalisation theories and models presented in Chapter 3. Rather than fixating on what makes online interactions different to offline ones, SAT seeks to assess how an individual's propensity to radicalisation (i.e. their vulnerabilities or stressors) interacts with their environment to affect their norm-based motivations – i.e. why do some individuals see terrorism as an acceptable (and often the *only* acceptable) form of action (Wikström and Bouhana 2017). It does not assume that propaganda will necessarily influence its audience, nor does it preclude it, but instead attempts to understand why certain predispositions and environmental factors may result in resonation for some but not others. Importantly, it relies on the importance of socialisation within certain settings, whether they are online or offline (Bouhana 2019).

Rejecting the simplistic online/offline dichotomy and instead taking a more holistic view helps to understand the differences between environments on different platforms. Halpern and Gibbs (2013) compare political discussion on Facebook and YouTube, finding that the sites' affordances have an important effect on deliberation. Facebook's

interconnectedness and lack of anonymity expands the flow of information and allows for symmetrical discussion, while YouTube, which is more anonymous and deindividuated, results in a less polite discourse. Presently, there is little research in terrorism studies that has taken a comparative approach to social media platforms and therefore we have little understanding of how the affordances and structural environments affect user experiences. We do not know how the Twitter user experience of timelines, 280 characters, and public audience compares to Telegram's invite-only groups, self-destruct messages, and relative lack of content moderation. Similarly, we have little knowledge of whether platforms are uniform in the ways they disinhibit users; or how they form of echo chambers, and importantly, how each of these may affect radicalisation trajectories. Research has shown that platforms' recommendation systems have different effects when it comes to promoting extremist content (Reed et al. 2019), suggesting that there may be important environmental differences between platforms. Rather than merely dividing them up into "online" and "offline" categories, it will be more fruitful to understand these platforms' user experiences in relation to each other. It is possible that there are more differences between some types of online communication than between online and face-to-face.

To demonstrate how such a theory could be utilised to better understand actors' information environments, this chapter will draw on a case study of Abdullahi Yusuf. This will firstly outline the difficulty in separating the online and offline aspects of his radicalisation before drawing from a SAT-inspired framework developed by Bouhana (2019) to demonstrate how a holistic theory of radicalisation can help to explain how communications technologies can create an information environment which affects an individual's norm-based motivations. The case study is not intended to be representative, but rather was chosen for the purposes of exposition. Yusuf's case study has particularly deep and rich data. Rather than speaking for the whole sample, it should be considered a vessel to demonstrate the limited analytic utility of an online/offline dichotomy compared to a theory which can account for the multiplicity of interrelated environments. However, it will immediately become clear that many of the overall findings and themes of this thesis are represented within this case study.

7.3.4 Abdullahi Yusuf and his Environment

Yusuf was an attempted traveller in the Minneapolis/St Paul area of Minnesota; part of a network of many individuals that either successfully or unsuccessfully attempted to fight with IS. He had deep ties with some members of this local network, including successful traveller Hanad Mohallim, whom he had been best friends with for several years previously.[341] According to Yusuf, Mohallim played an important part in his decision, noting that he had shown him online propaganda when the two were together in Minneapolis only a couple of weeks before Mohallim's travel in March 2014.[342] The two

[341] USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint; Temple-Raston. He Wanted Jihad. He Got Foucault.
[342] Temple-Raston. He Wanted Jihad. He Got Foucault.

kept in contact via phone and text message after the latter made it to Syria, helping provide Yusuf with operational support and a travel partner in Abdi Nur.[343] After Mohallim left, another network member – Guled Ali Omar – reached out to Yusuf to introduce him to the wider network of young Somalis in the area who, according to Yusuf, created a sense of brotherhood and belonging, as well as continuing his ideological development in group meetings by passing round cell phones and tablets to share radical videos with each other.[344] Individuals in this network were part of Yusuf's wider social network. Mohammed Farah and Abdi Nur went to his school, while others were members of his mosque.[345]

Yusuf cites several factors in his development towards engaging in terrorism. His network of co-ideologues provided him with propaganda which he suggests "mesmerised" him: 'It's like the message is for you. Get up off your butt if you don't like it. And, you know, it's just check, check, check, that's me, that's me, that's me'.[346] His peers also attempted to persuade him personally, giving him the ultimatum that they were going to travel in a few weeks and if he wanted to join them, it was now or never. Moreover, Guled Ali Omar framed their decision as a perilous and brave one: 'Abdullahi, we're on a long and hard journey. We're going to Syria to fight, and you can join us if you want to, but if not, if you turn around and walk away right now, there are no hard feelings,' to which Yusuf immediately agreed, noting that hesitation meant that you are not a true believer.[347]

Yusuf had other influences outside of his network of co-ideologues too. At around the same time that he was beginning to make friends with this crowd, his history teacher assigned him a presentation on the Syrian conflict, which he knew little about before. Upon learning about the atrocities against civilians and children committed by the Assad regime, he expressed moral outrage.[348] This helped his network of peers frame the issue as a morally justified one in which he would be doing sacred work and protecting innocents.[349] His parents may have also inadvertently affected his environment and pushed him towards his plot. When Yusuf began to spend more time with the radical network, his parents did not object because they thought he was merely becoming more religious, which they did not see as a bad thing.[350]

Yusuf also engaged on a range of social media platforms. His Facebook profile picture was a man depicted with a head of a lion – the notion of fighters as lions is common in jihadist circles (Williams 2011; Benedek and Simon 2020). He also posted comments such as

[343] Meleagrou-Hitchens, Hughes, & Clifford, The Travelers: American Jihadists in Syria and Iraq.
[344] Temple-Raston. He Wanted Jihad. He Got Foucault.
[345] USA v. Abdirizak Warsame, Criminal Complaint.
[346] Temple-Raston. He Wanted Jihad. He Got Foucault.
[347] Temple-Raston. He Wanted Jihad. He Got Foucault.
[348] Koerner, B.I., Can You Turn a Terrorist Back into a Citizen? *Wired*, Jan 24, 2017. Access via: https://www.wired.com/2017/01/can-you-turn-terrorist-back-into-citizen/.
[349] Koerner, Can You Turn a Terrorist Back into a Citizen?
[350] Temple-Raston. He Wanted Jihad. He Got Foucault.

"Bashaar asad don't deserve to live,"[351] which given his "research" into Syria and conversations with co-ideologues at the time, could be an example of performative identity for his network. As noted above, he accessed radical propaganda with his friends, via a YouTube channel called "Enter the Truth" which contained IS productions which focused on the suffering of Syrian children and the moral corruption of the West.[352] Yusuf described watching these videos as akin to "one more episode of Game of Thrones," finding himself awash in another reality in which he could be a noble warrior instead of a helpless bystander.[353] He was attracted to travel to Syria because of connections he had made on Instagram, having noticed fighters "having nice villas and nice cars and stuff like that."[354]

A cursory analysis of Yusuf's online activity may lead a reader to believe that he was radicalised online; he used the Internet at multiple stages to access content which he personally ascribed as changing his perspective and acting as a motivation for his travel. Alternatively, looking at his offline activity may lead one to believe he was radicalised offline – most notably his pre-existing and new face-to-face connections with local co-ideologues, which over several meetings fomented his decision to travel. However, attempting to choose between one or the other is not sufficient in explaining the dynamics in Yusuf's case. This type of thinking is demonstrated in research by Reynolds & Hafez (2017), who offer three hypotheses to explain the mobilisation of 99 German foreign fighters: a lack of integration, online radicalisation, or offline social networks. The research rejects the online radicalisation hypothesis because they believe it would produce geographically dispersed mobilisation rather than in clusters. Instead, they accept the offline networks hypothesis because of the high level of clustering around areas which include pre-existing social ties. In essence, they assume that strong offline networks are mutually exclusive to online radicalisation.

However, a closer look at the dynamics involved in Yusuf's case show that there is no clear online/offline dichotomy to be drawn. His peer network – largely made up of social selection relating to proximity and shared institutions such as school and his mosque – were physically present at many stages of interaction with online propaganda. They introduced him to the content, watched it with him during face-to-face meetings, and members kept him updated with messages from inside the caliphate after they travelled. Yusuf ascribes both online content and the conversations with his peers as being a motivator for travel – but importantly the two happened in an inseparable way. Any theory which purports to show why acting online is fundamentally different to acting offline cannot withstand scrutiny given the interrelatedness of the two domains. In short, rather than an either/or dichotomy, Yusuf's case demonstrates that the Internet can play an important role between members of tight-knit groups with deep social connections.

[351] USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint.
[352] Koerner, Can You Turn a Terrorist Back into a Citizen?
[353] Temple-Raston. He Wanted Jihad. He Got Foucault.
[354] Temple-Raston. He Wanted Jihad. He Got Foucault.

Figure 21 outlines the complex interplay between the different online and offline activities, showing that there is no easy demarcation to be drawn between the two.

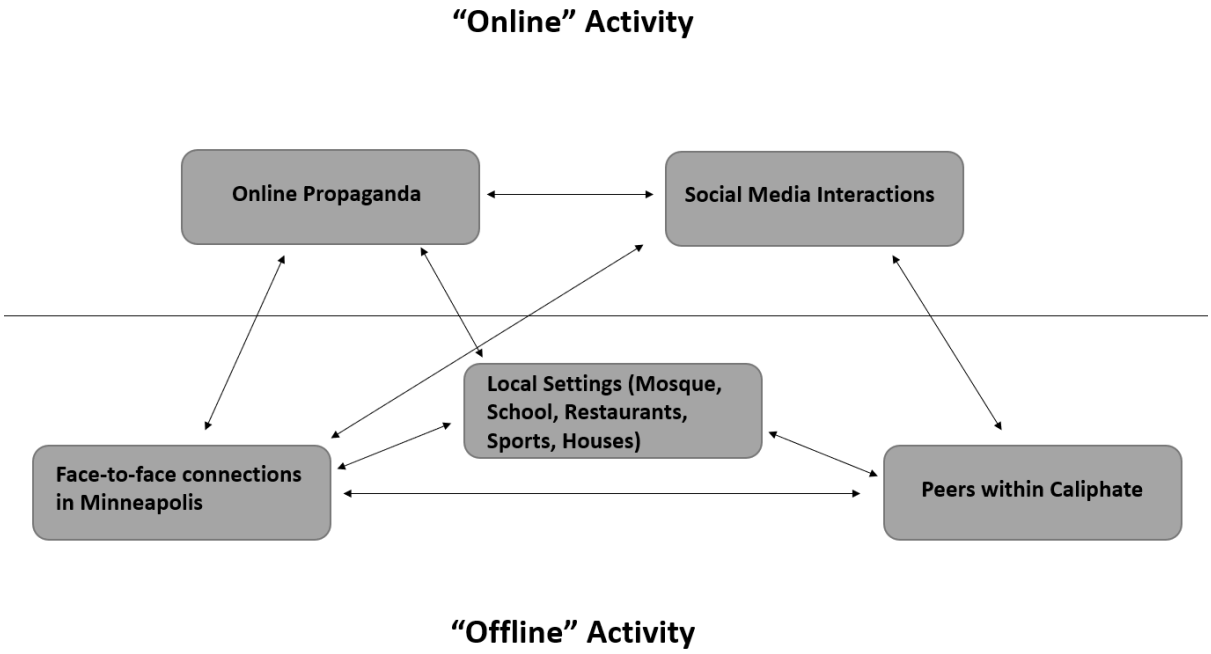


Figure 21 - Yusuf's Online vs Offline Activities

Using SAT to Understand Yusuf's Information Environment

Given that we cannot consider Yusuf's activities to be easily demarcated into either online or offline, it could be more fruitful to consider his combined information environment within a wider theory of radicalisation. Using Bouhana's (2019) *5S* framework, based on SAT, we can understand how Yusuf's information environment interplayed with other factors that affected his norm-based motivations to engage in extremist behaviour. The framework consists of five sets of factors which may play a role in facilitating (or failing to hamper) the emergence of extremism: *Susceptibility, Selection, Settings, Social Ecology,* and *Systems*. As Figure 22 demonstrates, these factors are mutually reinforcing, with *Susceptibility* and *Selection* leading to an individual's vulnerability, which if exposed to certain settings can lead to the facilitation of radical behaviour. The *Settings* both influence and are influenced by the *Social Ecology*, which in turn influences and can be influenced by wider *Systems*. The *Systems* can lead to the emergence of predisposing factors, linking back to *Susceptibility* (Bouhana 2019). This framework demonstrates that a holistic theory of radicalisation which encompasses both online activity, offline activity, and other personal and environmental factors offers a fuller explanation of Yusuf's trajectory. Importantly, in this case study, online activities can be seen in each of Bouhana's five sets of factors.

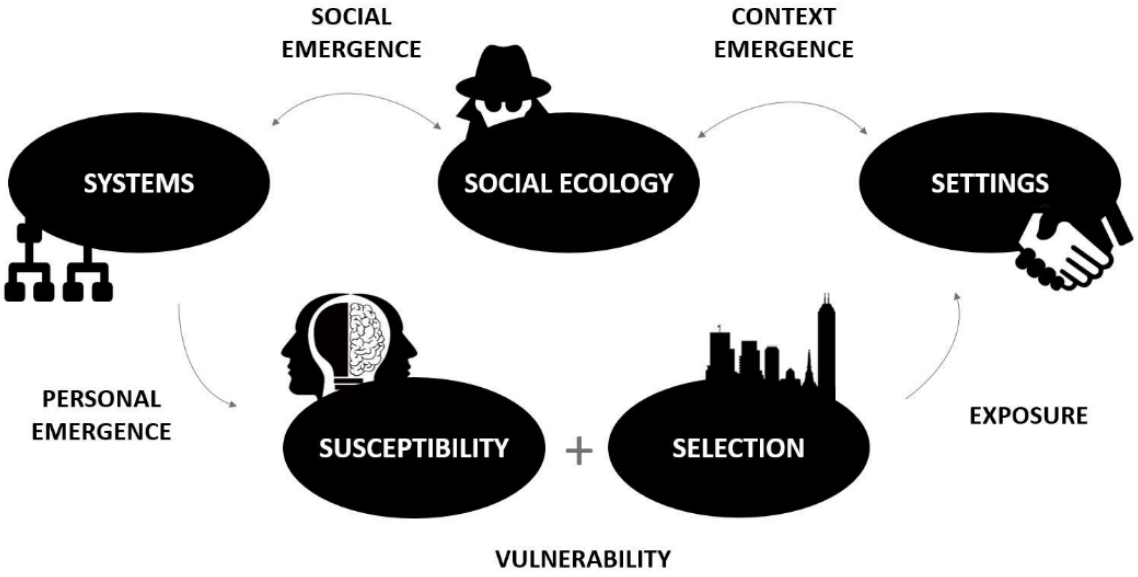


Figure 22 - Bouhana's (2019) S5 Inference Framework

To begin, Bouhana (2019) notes that individual *Susceptibility* is the key determinant to moral change. While it is difficult to establish every possible factor that could render an individual susceptible, particularly those at the subclinical level, several factors are apparent within Yusuf's case. He describes his motivation for travelling as being less about ideology and more about a sense of adventure, excited at the prospect that he was going to be part of ISIS' Special Forces or Navy Seals[355] – Bouhana (2019) describes thrill-seeking as having been linked as a determinant to crime. Importantly, Yusuf cites online propaganda as fulfilling this sense of adventure within him.[356] Bouhana (2019) also notes that a weak commitment to context-appropriate rule-guidance can be an important factor, which can be identified by having past criminal behaviour. Yusuf also grew up in a high-crime area of Minneapolis and socialised with friends who stole cars and engaged in recreational drugs, which he would eventually do as well.[357] His parents repeatedly moved him from schools to avoid a run in with the police.[358]

Mere susceptibility is not enough to predict engagement with extremism. Instead, several contextual factors can affect engagement. The idea of *Selection* is important in understanding actors' information environments and can be split into two parts. Social selection is dictated by the social forces that encourage (or discourage) individuals from engaging in place-based activities (Bouhana 2019). For Yusuf, his location is clearly important because it placed him in close proximity to a pre-existing network of

[355] Temple-Raston. He Wanted Jihad. He Got Foucault.
[356] Temple-Raston. He Wanted Jihad. He Got Foucault.
[357] Koerner, Can You Turn a Terrorist Back into a Citizen?; Temple-Raston. He Wanted Jihad. He Got Foucault.
[358] Temple-Raston. He Wanted Jihad. He Got Foucault.

extremists dating back a number of years.[359] Moreover, his school and mosque, both local to him, were key venues in which he made connections.[360] Self-selection describes how and where an individual chooses to spend their time. As described above, he chose to spend time with his new social network via basketball sessions and meetings in restaurants, but also engaged with these same individuals using online platforms. Social selection and self-selection are importantly interlinked; Yusuf's choice to spend time online was informed by his peer network, which was in turn heavily related to his location. The idea of selection bridges individual susceptibility and environment factors (Bouhana 2019); Yusuf's predispositions are likely shared by several individuals that do not engage in extremism, but his proximity to existing networks and choice to engage with them could have exacerbated his susceptibility.

The next set of factors are the affordances offered by the *Settings* that make up an actor's environment and provide norms which encourage extremism (Bouhana et al. 2016). Yusuf's environment offered him a range of moral affordances – 'discursive opportunities to promote ideas, which characterise extremist behaviour as morally legitimate' (Bouhana 2019; p. 16). His interaction with his co-ideologues, whom he watched propaganda alongside, created a moral imperative for him to travel to Syria, stating that he would be doing sacred work by saving women and children from the Assad regime.[361] This was exacerbated by the "now or never" ultimatum that his peers gave him, which Yusuf did not feel he could decline for fear of not being a "true believer."[362] The network also provided him with attachment affordances – the interpersonal process by which an individual forms attachments to radicalising settings (Bouhana et al. 2016). From an early age, Yusuf noted that he longed for a sense of belonging,[363] which was provided by the group of young Somali men: 'There was a real sense of brotherhood and belonging. It felt like they were welcoming me into something'.[364] Finally, there was lack of social control norms that could have possibly provided an intervention. His parents did not object to his new circle of friends; the basketball games which led to propaganda sharing were unsupervised; and his online activity took place at a time where extremist content was easily available on mainstream platforms prior to the regulatory fightback (Berger & Perez 2016; Grinnel et al. 2018; Conway et al. 2018).

An important factor interrelated to radicalising settings is the *Social Ecology*; the community-level factors that permit or restrict the emergence of radicalising settings (Bouhana, 2019). This, too, took place over both domains. The Minneapolis/St Paul area was not only a hot spot for travel to IS but had previously been a point of departure for many actors that travelled to join al-Shabaab between 2007-2012 (Vidino, Harrison, and

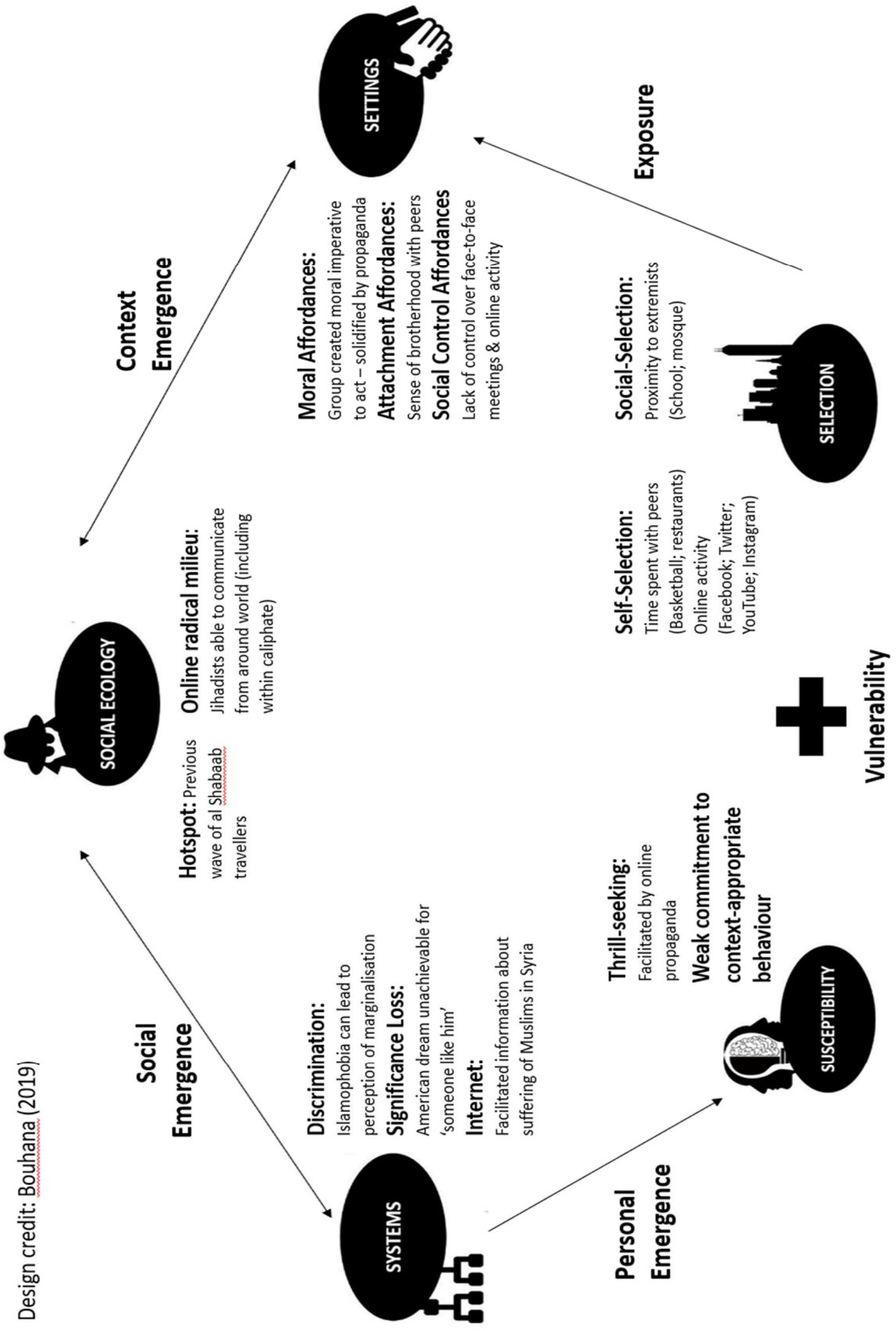
[359] Temple-Raston. He Wanted Jihad. He Got Foucault.
[360] USA v. Abdirizak Warsame, Criminal Complaint.
[361] Koerner, Can You Turn a Terrorist Back into a Citizen?
[362] Temple-Raston. He Wanted Jihad. He Got Foucault.
[363] Koerner, Can You Turn a Terrorist Back into a Citizen?
[364] Temple-Raston. He Wanted Jihad. He Got Foucault.

Spada 2016). In fact, Guled Ali Omar's brother had travelled in 2007.[365] In total, the FBI estimate that at least 45 left the area to join either al-Shabaab or IS, with a dozen more that were arrested attempting to leave.[366] This could have created a social ecology which placed its members within proximity to criminogenic settings which are outlined in the previous paragraph. Moreover, the Internet can provide an extremism-facilitating social ecology as well, particularly given the reach of IS sympathisers on mainstream platforms such as Twitter (Berger & Morgan 2015; Klausen 2015), Facebook (Carter et al. 2014), and YouTube (Shane 2016) at around the time of Yusuf's radicalisation, all of which Yusuf used.[367] One example of this is providing a platform (Instagram) for Yusuf to stay updated with foreign fighters, whose motivation was spurred by their villas and nice cars.[368]

The final set of factors is the *System*-level, which can promote the emergence of moral ecologies that support extremism. Bouhana (2019) notes that systemic processes that exacerbate discrimination can produce extremism supportive settings; Yusuf observed discrimination in his life on several instances. In school, he suffered bullying from both black and white classmates due to his Somali ethnicity. In second grade, he got into a fight with another child after the student removed a Somali girl's headscarf. Reflecting on growing up in the wake of 9/11, he noted that there was always a whiff of anti-Muslim bias in the air, often being the butt of terrorist jokes, which put a doubt into his head as to his place in American society.[369] This, and other, systemic factors can lead to perceived marginalisation and a feeling of insignificance (Bouhana 2019), which Yusuf also described, noting his poor upbringing made him feel that the American dream had become unachievable for someone in his shoes, making him wonder whether he truly belonged in the country.[370]

[365] USA v. Mohamed Abdihamid Farah et al.
[366] McKay, H., How Minneapolis' Somali community became the terrorist recruitment capital of the US, *Fox News*, Feb 16, 2019. Access via: https://www.foxnews.com/us/how-rep-ilhan-omars-minnesota-district-became-the-terrorist-recruitment-capital-of-the-us-officials-highly-concerned.
[367] USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint; Koerner, Can You Turn a Terrorist Back into a Citizen?
[368] Temple-Raston. He Wanted Jihad. He Got Foucault.
[369] Koerner, Can You Turn a Terrorist Back into a Citizen?
[370] Temple-Raston. He Wanted Jihad. He Got Foucault.

Figure 23 - Yusuf's 5S Framework



The Internet also plays an important role in systemic level factors. Bouhana (2019) notes that communication technologies can expose individuals to information about the treatment of other groups, which can increase the possibility for friction or perceptions of relative disadvantage. Yusuf reported exactly this; his history project caused him to actively search for the events in Syria which highlighted the suffering of Sunni Muslims at the hands of the Assad regime, which in turn caused him to express moral outrage.[371] This was at the same time that he began to socialise with his wider network of co-ideologues at his mosque, who framed IS as undertaking sacred work by protecting innocents in Syria.[372] The Internet has been important in changing this dynamic; typically in the past conflicts were localised, but online communication has multiplied sources of friction and fostered ideological ties even if actors are geographically distant (Bouhana 2019).

Theories of online radicalisation have tended to focus solely on how online technologies affect radicalisation (Bastug, Douai and Akca 2018; Neumann 2013a; Weimann and Von Knop 2008) or have attempted to show why acting on the Internet may be fundamentally different to acting offline (Ducol et al. 2016; Koehler 2014; Saifudeen 2014; Torok 2013; Sageman 2008). However, at both the empirical and ontological level, the online/offline dichotomy cannot withstand scrutiny. In essence, there is no analytically useful theory of online radicalisation. Given this, if one wishes to understand the role of communications technologies within terrorists' trajectories, it is prudent to assess their role within a broader, holistic theory of radicalisation. To this end, Bouhana's SAT-inspired 5S framework offers micro, meso, and macro-level factors which can contribute towards the emergence of extremist behaviour. Importantly for the objectives of this thesis, it does not rely on an online/offline dichotomy but rather flourishes in the complexity of different information environments. In Yusuf's case, it does not matter whether watching and discussing online propaganda with peers, or whether keeping in contact with pre-existing social networks once they travelled to the caliphate via social media, is treated as an online or offline activity. Instead, the focus is ascertaining how these interactions, and wider environments, affected Yusuf's motivations to travel to IS.

This section drew from Yusuf's case study to demonstrate how Bouhana's framework can be deployed to assess the role of the communications technologies in cases of terrorism without having to rely on the false online/offline dichotomy. As noted at the start of this section, the case is not intended to be representative of this sample or wider terrorism populations; there will doubtlessly be cases which have a much heavier emphasis on communications technologies as well as cases in which they play a considerably smaller role. Rather, it is intended as a jumping off point to move beyond theories of online radicalisation and highlight a framework which analyses the role of communications technologies in a wider context.

[371] Koerner, Can You Turn a Terrorist Back into a Citizen?
[372] Koerner, Can You Turn a Terrorist Back into a Citizen?

7.4 Policy Contribution – The Fragile Ecosystem and Unintended Consequences

The previous section has demonstrated that there is little value in strictly demarcating the online and offline domains when it comes to terrorist activity. However, policy responses to date seem to be making this exact assumption. As Gill et al. (2017) note, policy debates tend to be focused upon a specific location – particularly the Internet. This has led to the proliferation of proposed regulation such as the Online Harms White Paper (HM Government, 2019) and the EU's Digital Services Act (2021), which emphasise the risk of the Internet. Corner and colleagues note that: 'public discourse, government bodies, and the media all reinforce the perception of the danger posed by online environments, which are presumed to be ripe for exploitation by radicalizing agents' (Corner, Bouhana and Gill, 2018, p. 28). However, as both this and other research suggests (von Behr *et al.*, 2013; Gill *et al.*, 2017; Reynolds and Hafez, 2017), this is not an easy distinction to draw. If policy focuses primarily on online interactions, then they run the risk of missing the environmental interactions which shape norm-based motivations, as discussed in the previous section.

In recent years there has been a clear move towards more stringent regulation of terrorist content on the Internet, particularly in Europe. The European Parliament has passed a proposal which states that Internet companies should remove content within an hour of receiving a notification from law enforcement, with those that persistently breach this target being fined up to 4% of the company's turnover (EU Parliament 2019). Similarly, the UK Government published its *Online Harms White Paper*, which includes tackling terrorist content. The white paper suggests several regulatory approaches, which include platforms potentially being blocked and members of senior management being held legally accountable (HM Government 2019). Similarly, after the terror attack in Christchurch, New Zealand in March 2019, Prime Minister Jacinda Ardern and French President Emmanuel Macron led the "Christchurch Call", an action plan which commits several actors to a range of measures to achieve the ultimate goal of the elimination of terrorist content online (Ardern 2019). The Call was adopted by 10 countries, including France, the UK, and Canada, as well as the European Commission. The Global Internet Forum to Counter Terrorism – which includes Facebook, Google, Twitter, Microsoft, and Amazon – also supported the Call, offering several steps they were taking to remove terrorist content (Global Internet Forum to Counter Terrorism 2019). Initially, the US did not sign up to the Call because of its commitment to defend the First Amendment (Alexander 2019), but eventually joined in May 2021 (Christchurch Call nd).

An important finding of Chapter 5 was the negative correlation between using the Internet and the success of an event. That is to say, the actors who used the Internet to communicate with co-ideologues or to prepare for their event were less likely to be successful than those that did not. This is instructive because one may infer that terrorists' use of the Internet may actually be aiding law enforcement; a number of actors in the sample telegraphed their intentions on social media platforms, which led to law enforcement opening investigations. The inference that can be made here is that using

the Internet may be a hindrance, rather than a help, to those that wish to conduct acts of terrorism. This supports the research by Jensen, James, et al. (2018) who find that US-based actors that use social media have lower success rates than those that do not. They also find that 'activity on open social media platforms, such as Facebook and Twitter, played a key role in the identification and interdiction of U.S. foreign fighters and terrorism suspects in several recent cases' (Jensen, James, et al. 2018, p.1). The notion that Internet usage may be a hindrance also partially supports Gill and Corner's (2015) study of UK-based lone actor terrorists, finding that individuals that learned about or planned their event online were significantly less likely to kill or injure a target.

This leaves a difficult policy dilemma. Identifying potential terrorists online is undoubtedly an easier task on larger social media platforms such as Twitter and Facebook, which have an open or semi-open site architecture in which agents can more easily identify actors. The findings of Chapter 5 suggest that using encrypted social media platforms is net neutral in terms of safety – i.e. no significance was found in event success between those that use it and those that did not. When compared to the significant relationships in other online behaviours discussed above, it suggests that using end-to-end encryption does not provide cast-iron protection, but it may be a safer way of operating online. Another important factor is that the big tech companies are more likely to be compliant to subpoena requests compared to sites such as Telegram who do not comply with government and law enforcement demands (Clifford and Powell 2019; Bloom et al. 2017). This non-compliance, along with other factors such as end-to-end encryption, pseudo-anonymity, and temporary external links (Bloom et al. 2017) offers substantial security benefits over the mainstream platforms. It could be, therefore, that by forcing actors away from mainstream platforms where they can be detected more easily by law enforcement, onto more secure ones, content removal policies are inadvertently helping terrorists.

To make matters more complicated, the findings of the same chapter downplayed a potential migration from mainstream social media platforms to end-to-end encrypted ones. Taken year-by-year, terrorist actors in this sample were just as likely to use encrypted apps in 2012 as they were in 2018. This is a particularly interesting finding because it is at odds with much of the literature in the "supply-side" of online terrorism research, which posits a migration of IS supporters to such platforms, particularly Telegram (Clifford and Powell 2019; Bloom et al. 2017; Prucha 2016; Conway 2018). Given this disparity, it is important to further research the prevalence with which terrorist actors use encryption, which will be discussed in the section on future research below.

Even if content removal hinders law enforcement detection and investigations, there are clear benefits too. Terrorist groups – and IS in particular – have been successfully degraded online by suspensions and removals. Two studies by J.M. Berger and others elucidate this point well. In research conducted in 2014, Berger and Morgan conducted a social network analysis of IS supporters on Twitter, finding that there were between

46,000 and 70,000 sympathisers on the platform and that a small group of 500-2000 hyperactive accounts were able to successfully spread the group's message far and wide (Berger and Morgan 2015). In research conducted a year later, Berger and Perez found that suspensions were drastically limiting the reach of the group on the same platform. They found that there were between 1,000-3,000 English language accounts. Importantly, they found that although accounts were being again set again up after suspensions, it had a devastating effect on users' followers (Berger and Perez 2016). Other recent research has also highlighted that suspensions and content removal has degraded the group online (Conway et al. 2018; Grinnell et al. 2017). Given the host of affordances and opportunities that the Internet offers, such as cheap communication between actors across the world or recruitment via social media platforms, which this research shows terrorists are utilising, degrading actors' ability to use these platforms is clearly a desirable policy goal.

Although content removal should certainly be an aspect of the policy response to online terrorist content, others have suggested alternative routes, too. Alexander and Braniff (2018) suggest a middle ground of marginalisation. They argue that the current system of content removal is tantamount to a game of "whack-a-mole" because it relies on platforms which are compliant with takedown requests, forcing those in the online radical milieu to migrate to new platforms, which are not. Rather than attempting what they argue is an untenable goal of removing all terrorist content from the Internet, Clifford and Powell (2019) note that marginalisation seeks to contain extremist actors where it is difficult for them to reach the public and yet still possible for law enforcement to detect, monitor, and investigate them. Rather than driving them away from mainstream platforms, the idea is to restrict their connectivity to the wider non-radical network. To borrow an analogy from drug policy research, it is the difference between models of prohibition, which seeks to stop all drug use, and harm reduction, which accepts that individuals will continue to use drugs and seeks to eliminate undesirable consequences. These actors will then be more detectable for both law enforcement and CVE initiatives, such as the Redirect Method (Google 2016), public communication campaigns (Tuck and Silverman 2016), or one-on-one interventions (Frenet and Dow 2018). Furthermore, keeping actors on platforms that are compliant with subpoena requests, unlike Telegram, can be vital in the process of building a case.

This is a complex and nuanced policy problem. There are clear benefits to removing terrorist content from the Internet and there are a host of incentives and disincentives that go beyond security – i.e. even if not illegal, social media platforms may deem this content distasteful and therefore bad for business and it is not reasonable to compel them to keep it on their sites. Furthermore, there are important freedom of speech and rule of law issues that go beyond the scope of this research when considering content removal. At a more abstract level, this plays into the wider philosophical question of whether content prohibition should be a utilitarian judgement based on harms and trade-offs, or a position based on the morality of the content. That being said, the contribution of this research to the debate is to offer an empirical insight that the current direction of travel

in online regulation of terrorist content may end up being harmful in the long-run (if specific harms are able to be quantified). At the very least, it offers a fuller understanding of some of the unintended consequences and trade-offs that come with content removal and shows that there are other paradigms beyond pure removal.

7.5 Limitations

Although it is well-reasoned to analyse a group such as IS given the unprecedented geopolitical threat they posed, focusing on a single group or ideology runs the risk of treating a phenomenon as homogeneous when, in fact, different groups may yield substantively different behaviours. This has been mitigated, to some extent by comparisons against cross-ideological research that has similar variables – but leaves open the possibility of differences in subjective coding (discussed below). In a similar vein, Chapter 3 identified that the vast majority of research into the demand-side of online terrorism was Western-centric, which this thesis does not remedy by focusing on a US-based population. Although comparing between groups or locations can lead to instructive findings, the nature of this project makes it unfeasible. Data collection and analysis for the 201 actors in the sample took over a year to complete, therefore, to increase the scope of the project would not have been possible. Despite this, the findings offer important empirical contributions which can be used as a basis of comparison for other scholars' future research.

Another limitation is a lack of base rates. Gill (2016) notes that 'we have no grasp on the societal prevalence of the vast majority of online radicalisation indicators… Behaviours, like making threats online, are a…difficult task to quantify' (Gill 2016, pp.6–7). For some factors, such as broad Internet usage or preferred social media platform, the sample has been compared against the US population, but for others it is not possible to compare the online behaviours of terrorists against the general population, which remains a substantial gap in understanding the role of the Internet. Relatedly, the lack of a control group of nonviolent radicals, as used by Bartlett and Miller (2012), means that the research is not able to discern the relationship between those that engage in violence or with other terrorists and with those that do not.

More broadly, utilising secondary sources has clear limitations. Access to primary data on terrorists is a longstanding problem within the field on account of both ethical and practical considerations (see, for example: Victoroff 2005; Thornton and Bouhana 2017). The original authors of court documents, academic and government reports, and journalistic sources did not intend for their work to be used as data for a study into the online behaviours of terrorists. Rather, they were writing to fulfil their own goals such as selling newspapers or setting out reasons for convictions. As a result, there is a not-insignificant amount of missing data; the considerations for how to mitigate this can be found in the methodology. Schuurman (2018) highlights this problem, particularly in the context of database studies such as this one noting that research that is based on journalistic sources can suffer from factual inaccuracy, editorial bias, and the

underreporting of failed or foiled terrorist attacks. Utilising secondary sources carries an assumption that the original author collected their data in a relatively robust manner, which as Schuurman notes, is not always the case, and therefore a limitation to this research.

The combination of several different types of sources mitigates this problem to some extent. Behlendorf, Belur, and Kumar (2016) demonstrate that database studies with a single data source may miss several terrorist events, while Chermak et al. (2012) show that some attacks are more newsworthy than others, which can affect data collection in studies such as this one. In this sense, the different sources are complementary. The data from court documents offer a granular-level account of the behaviours that actors exhibited in the direct run-up to their event, which can be supplemented by journalism which engages with interviews with friends or family, or in some cases, the terrorist themselves. Similarly, academic material can offer a layer of quantitative and qualitative analysis, while also offering theoretical contributions. Finally, there is a considerable benefit to the use of secondary sources; the behaviours that are mentioned are referenced, meaning that they can be checked by others for academic rigour. Studies with primary sources, for example interviews, often rely on the singular direct interpretation of the researcher which is not referenced.

The final limitation is that coding is subjective – addressed in the quantitative analysis when comparing the results of this research against that of Gill et al. (2017). Many studies of terrorist behaviours are able to utilise a system that uses two coders, which can then be tested for inter-rater reliability. The nature of a doctoral thesis makes this impossible. The inclusion of a second round of quantitative coding mitigates this to some extent, offering the opportunity to look again at the data months after the original code. Furthermore, the thought process behind the GTM coding was elucidated in the methodology and referenced in the analysis. Despite these limitations, this thesis offers an important empirical contribution to the current understanding of online radicalisation.

7.6 Future Research

This thesis has made three contributions to the online radicalisation literature: an empirical understanding of terrorists' pathways and the role of the Internet; three levels of theoretical abstraction for understanding online radicalisation (the radicalisation dynamics, the ontological challenge, and the addition to the theoretical framework); and a policy contribution regarding the fragile ecosystem in what terrorists operate. There are several avenues by which this project can be continued and advanced. These include: testing the theoretical contributions outlined above; analysing the sequences with which terrorists act as part of their antecedent behaviours; comparing the different affordances that social media platforms offer; analysing the effects of propaganda from consumers' perspectives; as well as continuing to test in the future to see if the findings presented

above change such as assessing whether there is a more widespread migration towards end-to-end encrypted platforms by terrorist actors.

7.6.1 Theoretical Contributions

As noted in Chapter 6, the purpose of GTM is not to test existing findings but generate theory grounded in the data which can be tested and explored further. There are several different ways in which future research could expand upon the radicalisation dynamics that emerged from the data. For example, there are few studies that empirically study the role of propaganda from an audience and prosumer perspective (Conway 2016a). Chapter 6 found that it plays an important role in a socialising radicalisation process, which could be investigated using primary sources in future. Interviews could be used to establish what types of conversations and meetings were had around the consumption of propaganda and whether group-based activities spurred individuals towards more extreme content. This chapter also found that female terrorists used online technologies to carve out a space for themselves to build a less restricted identity. However, the sample of females in this analysis was only twenty so should be analysed using a deeper pool of terrorists to assess whether this mechanism still holds. Finally, the chapter found the Internet to be akin to a buyers' market in which individuals use the Internet to gratify their needs. This line of research could be expanded upon by analysing actors' Internet usage via Google search and social media data. In some cases in this sample, the court documents give great depth of detail as to what individuals searched for and when. With a detailed dataset, this could be expanded upon to gain a better understanding of *exactly* when individuals turned to the Internet and what was happening in their life at the time.

As proposed above, SAT can be used to better understand the information environment that actors inhabited, and in turn, how it affected their norm-based motivations to ultimately commit acts of terror. Rather than merely attempting to assess online behaviours, or even taking it one step further and assessing online and offline behaviours combined, this theoretical approach offers a more holistic understanding that operates at the micro, meso, and macro level – or in other words understanding the relationship between individual and context (Bouhana 2019). There is less need to establish whether an individual "radicalised online" or not than there is to understand an individual's propensities, selection choices, and the system in which they operate. Of course, online platforms likely play an important role in such systems, but this role should be taken in the wider environmental context.

7.6.2 Sequence Analysis

When planning this project, one avenue of investigation for online radicalisation was the speed of actors' trajectories. One of the five hypotheses of the von Behr et al. (2013) study is that the Internet accelerates the process of radicalisation, for which they did not find support. Importantly, they note that because there is no agreed length of time or template for radicalisation, 'it is hard to ascertain whether or not the internet accelerated the process of radicalisation' (von Behr et al. 2013, p. 28). More recently, Jensen, James, et al. (2018) found that individuals' trajectories are becoming faster as social media has

become more ubiquitous, although they note that there is a high degree of variance. Klausen et al. (2016) attempt to assess the length of actors' trajectories, which they define as the first engagement with extremist ideas to "bang", which is similar to the qualitative coding used in the section on online only trajectories in this research. However, as laid out in that section, this is problematic as a starting point of the radicalisation process because it ignores any number of stressors or vulnerabilities that could exist long before interaction with radical ideas. It also does not rule out false positives; it is entirely possible to interact with extremist content before beginning the process of becoming a terrorist. When analysing the data generated for this project, it became clear that the unevenness of the data would lead to a large number of cases being skewed. The court filings are heavily focused on the behaviours that directly preceded the event and therefore a number of cases, particularly those without data on actors' early lives, would show a far shorter trajectory which would likely be inaccurate.

Rather than focusing on time, a potential avenue for future research is sequence of trajectories, attempting to assess the order in which vulnerability indicators – including online behaviours – took place. This is the next logical step from the data that emerged in Chapter 6 which analysed online only trajectories and first steps into the movement. This has been utilised – outside the context of the Internet – by Corner, Bouhana and Gill (2018), who focus on the sequence of behaviours which characterise lone actor terrorist trajectories. This is important because much research in terrorism studies tends to focus on static variables, rather than considering them within a wider sequential context. Corner and Gill (2019) offer a similar methodology in their study of psychological distress and terrorist engagement. As well as judging the average trajectory time, Klausen et al. (2016), also sequence the events they are coding in an attempt to build a dynamic behavioural model of radicalisation. Importantly, this type of research must take a holistic view of the process, rather than focus on one factor, such as use of the Internet. However, there are still data-related problems when using this methodology. Corner, Bouhana, and Gill (2018) note that using open-source data may be insufficiently granular to draw firm conclusions, and Klausen et al. (2016) note that making reliable inferences using such data is demanding and relies on coder inference – which is not desirable for replicability. One solution could be to include a higher bar for evidence given that a number of actors have considerable information available, although this leaves room for skewed results. Another is to use different data, such as closed-source police files or first-hand interviews, which can be more granular and systematic.

7.6.3 Social Media Affordances

Another of the hypotheses in the von Behr et al. (2013) study of online radicalisation was that the Internet acts as an echo chamber for terrorists, which they define as 'a place where individuals find their ideas supported and echoed by other like-minded individuals' (von Behr et al. 2013, p.xi). They find support for this hypothesis in the majority of cases. This is an interesting hypothesis because it is the only one of the five in the study which relates to the architecture of online platforms affecting radicalisation,

such as chatrooms providing the illusion of strength in numbers. The experiences that different platforms' structure and procedural rules can provide are of great importance in understanding how individuals opt for violence. For example, there has been a great deal of research into IS' use of Twitter (for example, see: Prucha and Fisher, 2013; Klausen, 2015; Huey, Inch and Peladeau, 2017) and also research that has documented its move towards Telegram (Bloom et al. 2017; Prucha 2016; Clifford and Powell 2019), but there remains little comparing the affordances that each platform offers to users and how this may affect actors' trajectories. Conway (2016a) argues that research into violent extremism online should "compare" the differences between social media platforms in this way. Important questions include: How does a closed, invite-only chat compare to an open Twitter dialogue, which anyone can potentially see? How does the lesser fear of suspension affect the tone and content of discussions between co-ideologues? Research outside of terrorism studies has found that platform architecture affects discussion on Facebook and YouTube because of differences in anonymity, user-symmetry, and deindividuation (Halpern and Gibbs 2013).

Conducting this research using the types of open sources used in this study is impossible; although court documents do often show aspects of users' posting history on social media, they do not do so in a systematic manner and therefore the data are not granular enough. However, many other avenues exist to research social media affordances, such as digital ethnographies, as advocated by Conway (2016a) and utilised by Hegghammer (2014). Another strand of research into social media affordances is assessing the role of personalisation algorithms and violent extremist content, which has recently been undertaken by Ribeiro et al. (2019) and Reed et al. (2019) who both find that YouTube recommender systems can potentially lead users towards more extreme content. To further understanding of terrorist pathways, research needs to better understand how actors use recommender systems, rather than what would-be terrorists could potentially see, i.e. it needs to study the "demand" side rather than the "supply" (Von Behr et al., 2013).

7.6.4 The Future

There are several findings presented above that could, and may be expected to, change in the near future. Firstly, Chapter 5 downplayed a potential "displacement effect" in which, as mainstream platforms such as Facebook and Twitter took a more robust line of content removal and suspension towards IS sympathisers, actors migrated towards more secure, end-to-end encrypted platforms such as Telegram. Rather, it found that actors were just as likely to use end-to-end encryption in 2012 as they were in 2018. On one level, this is unsurprising as IS have continually maintained that they wish to remain on the larger platforms to reach as wide and organic an audience as possible (Berger and Perez, 2016; Clifford and Powell, 2019). However, one may reasonably expect that given continued improvements in social media platform and law enforcement detection, as well as knowledge sharing initiatives such as the GIFCT (Global Internet Forum to Counter Terrorism nd) and Tech Against Terrorism (Tech Against Terrorism nd) that this may

change in future. Recent research has shown that IS sympathisers have adapted by using different types of content for different parts of their communication strategies (Fisher et al. 2019), and a logical next step for this research is to understand how those that commit – or are arrested attempting to commit – acts of terrorism engage with a more hostile online ecosystem.

Chapter 8: Conclusion

This project began with a desire to better understand the phenomenon of "online radicalisation" in the era of social media. It was prescient because, in recent years, the world has seen the rise of one of the biggest and most dangerous terrorist organisations – IS – who conducted numerous attacks and to whom tens of thousands of individuals travelled to join. The group is particularly noteworthy because their online communication strategy was repeatedly described as sophisticated and wide-reaching, leading to the inevitable suggestion that individuals had radicalised online when they joined the group or acted on its behalf.

8.1 Summary and Key Findings

While this thesis is empirical in nature, each chapter is required as a separate step in successfully conceptualising and analysing the phenomenon under study. Chapter 2 highlights the conceptual ambiguity surrounding the word "radicalisation" – different scholars use it interchangeably to denote the process of becoming a terrorist, extremist, and radical. The key difference is whether it denotes a behavioural or cognitive process. These problems spill over into the conceptualisation of "online radicalisation" too and add to extra ambiguities surrounding what constitutes being sufficiently "online." There have been many attempts to theorise and model the process of radicalisation, although they tend to remain in the theoretical realm and have not been subjected to rigorous testing. Despite this, there is a growing literature which empirically analyses radicalisation; although there is no common pathway or terrorist profile, certain demographic, socioeconomic, personality, and experiential factors may appear more frequently than one would expect in the general population.

Chapter 3 surveys the existing literature on online radicalisation. As with the literature on radicalisation more generally, several scholars have attempted to theorise or model the process. These theoretical contributions have not yet adequately explained how the Internet affects radicalisation; most assume (or explicitly state) problematic assumptions, such as a relationship between engaging with radical content and becoming a terrorist or an ontological distinction between the online and offline domains. Empirical research into the "demand" side of online radicalisation tends to demonstrate that if one understands the process as the Internet replacing offline interactions in pathways towards terrorism, then it has not become the new norm. Rather, online and offline dynamics tend to complement each other. However, other findings suggest that the Internet may provide an important space for the construction of a radical identity, which may be fundamentally different online than off. An analysis of the literature on the "supply" side of terrorist content shows that up until around 2016, IS ran one of the most sophisticated and wide-reaching propaganda campaigns – primarily online – of any terrorist or extremist group in history. This highlights the importance of undertaking

data-driven research on IS actors to establish whether they are more reliant on the Internet than previous cohorts of terrorists, and if so, in what ways.

Chapter 3 concludes by establishing four research questions derived from the academic literature which are used for the quantitative analysis in the thesis: i) How frequently do terrorists use the Internet, and in what ways? ii) Has the online domain replaced the offline as the primary venue for radicalisation? iii) Do terrorists that act online demonstrate different experiences to those that do not? iv) Does acting on the Internet help or hinder terrorists?

Chapters 2 and 3 show that there are several conceptual problems underlying the study of contemporary pathways towards terrorism and the role of the Internet. Chapter 4 lays out the methodological groundwork for studying the phenomenon robustly and empirically. Rather than a focus on an ill-defined, abstract concept, it focuses specifically on discrete and observable behaviours collected from open sources. The chapter outlines the research design, methods of data collection, inclusion and exclusion criteria, the coding system, the methods of analysis, as well as ethical considerations.

Chapter 5 undertakes a quantitative analysis using a codebook developed from the academic literature to answer the four research questions outlined above. Before this, a demographic snapshot of the sample is presented which suggests that terrorist actors come from a range of backgrounds and life paths. However, as with the existing literature, commonalities appear; the sample is predominantly male, young and errs on the lower end of the socioeconomic spectrum. Converts appear to be over-represented, as do those with a criminal record. The findings of RQ1 suggest that the Internet is ubiquitous in contemporary terrorist pathways; actors used the Internet for a wide range of antecedent behaviours across several online platforms. Comparison with similarly coded studies suggests that terrorists may be using the Internet more than in previous years. Building on this, RQ2 finds that there is little reason to believe that online radicalisation is replacing offline; terrorists that engaged in a range of antecedent behaviours were significantly more likely to also act offline too.

Although the findings of RQ3 were more mixed, they generally pointed towards a similar experience for individuals that use the Internet and those that do not. For example, lone actors were *not* more likely to use the Internet than group-based ones, neither were individuals that plotted more sophisticated attacks. Finally, RQ4 shows that using the Internet may actually be hampering would-be terrorists' plots – individuals that acted online were less likely to be successful than those that did not. Taking all four RQs together, this chapter demonstrates the complexity of the relationship between terrorism and the Internet. One may be inclined to observe that most terrorists use the Internet as part of their plots and take that to mean they are radicalising online. However, Chapter 5 underscores the importance of offline interactions and the interrelated nature of the two domains.

The quantitative analysis of Chapter 5 provides an important overview of the sample as a whole. Chapter 6 supplements this with an inductive analysis of the sample's online behaviours using a methodology inspired by Grounded Theory. While Chapter 5 is limited to a codebook which mostly consisted of binary yes/no answers, this chapter explores emergent themes which are grounded in the data and derives three radicalisation dynamics. Firstly, rather than being seen as a direct motivator to act, terrorists' consumption of propaganda can also be seen as an ongoing socialisation process in which actors engage with the radical milieu to network, discuss, and construct radical identities. Secondly, for radicalising females, the Internet may offer a space for them to perform a less restricted gender identity than offline Salafi jihadist networks would allow. Finally, the vast information abundance of the Internet offer would-be terrorists a "buyers' market" to fulfil their needs in a flexible and constraint-free way. Taking these findings together, Chapter 6 reinforces the notion that radicalisation is invariably a social process; concepts such as self-radicalisation are largely redundant because even when acting online, terrorists are attempting to communicate, befriend, and network with others. The chapter also demonstrates the malleability of the online space – individuals are free to act with fewer limitations and build identities which reflect this freedom.

Finally, Chapter 7 synthesises the thesis into its original contributions. This thesis makes an important empirical contribution by adding to a nascent literature of data-driven studies which analyse the role of the Internet in contemporary radicalisation. Moreover, it draws from a complementary mixed method approach which goes beyond simply looking at online behaviours, instead considering them in relation to offline factors. There are also theoretical contributions at three levels of abstraction – the radicalisation dynamics established in Chapter 6; an ontological challenge based on the false dichotomy of attempting to separate online from offline activities; as well as demonstrating why a more holistic view of radicalisation – Bouhana's (2019) 5S framework – is a better tool for understanding the use of the Internet than existing online radicalisation theories. Chapter 7 then discusses the main policy contribution of this thesis, that the radical jihadist ecosystem is fragile and existing policy solutions may have unintended consequences that are harmful in the long run. After highlighting these contributions, it turns to the limitations of the study, which include focusing specifically on a single group and country; a lack of measurable base-rates for comparisons; the use of secondary sources; and the subjective nature of coding. Chapter 7 finishes by discussing avenues for future research, including testing the hypotheses which are generated in Chapter 6, analysing terrorist pathways via sequential analysis, researching social media affordances, as well as looking to the future to establish if new trends emerge.

8.2 Informing Policymakers and the Media

Despite this thesis and previous research pointing towards online radicalisation as a complex process, there is a need for these findings to inform decision makers and those with platforms that can effectively communicate these contributions to the public. As discussed above, popular media outlets often ascribe the Internet with radicalising

agency, as if there is something inherent which can dramatically alter an individual's trajectory. As both the empirical findings of this research and the review of the literature in Chapter 3 demonstrate, there is little reason to believe this is the case. Filter bubbles and online echo chambers do exist, but we do not know enough to say if they exacerbate individuals' pathways; terrorist propaganda is plentiful but the evidence-base for experimentally testing whether it is effective is still in its infancy. On the other hand, this research and others' has repeatedly highlighted that online interactions may be overrated in importance. However, the message that is often relayed to the public, via the media, is one that is confident that the Internet poses a substantial threat. Headlines such as "YouTube, the Great Radicalizer" (Tufekci 2018) or "Beware the Rabbit Hole of Radicalization" (Washington Post Editorial Board 2019) in the *New York Times* and *Washington Post* respectively are relatively typical of a narrative which not only places the Internet as the primary venue for this process, but often suggest that it has been some kind of "game changer" for terrorism.

This line of thinking is seemingly mirrored by policymakers, particularly in the United Kingdom, whose government recently published their *Online Harms White Paper*, which warns against 'terrorists, including Islamist groups such as [IS] and [AQ] as well as far right terrorists, [who] use the internet to spread propaganda designed to radicalise vulnerable people' (HM Government 2019, p.11). The white paper suggests that platforms that do not do enough to prevent this type of content could be faced with fines, ISP blocking, and criminal liability for executives. Similarly, in 2019, the UK Parliament passed a bill which increased the maximum sentences for terrorism precusor offences such as the dissemination of propaganda from seven to fifteen years (Counter-Terrorism and Border Security Act 2019). In February 2020, the Home Secretary said she was looking to "toughen up" these laws by creating a new offence of possessing terrorist material (Siddique and Grierson 2020). To be clear, there is a debate to be had over the virtues and pitfalls of removing terrorist content from the Internet that goes beyond the scope of this research. However there is little reason to believe that, as the *Online Harms White Paper* implies, that it will reduce terrorism. Rather, this research suggests that terrorists' ability to operate on the Internet may help law enforcement's investigations against terrorists. Moving forward, it is important for researchers to communicate nuanced findings to interested parties such as the media and policymakers so they do not create detrimental unintended consequenses or end up giving undue focus to one specific aspect of a much larger picture.

8.3 Towards an Evidence-based Understanding of Terrorist Pathways

Scholars have long lamented the dearth of empirical data which analyses the role of the Internet in pathways towards terrorism (Gill et al. 2017; von Behr et al. 2013). Rather than study the individual trajectories of terrorists – i.e. the demand-side – research into terrorists' use of the Internet has largely focused on the supply of content available to terrorists online. While this research is valuable and has informed this project, an over-reliance on the supply of content leaves a gap in the body of literature. This gap is

understandable, it is far easier for researchers to study online content – which terrorist groups often go to great lengths to make publicly available – than to wrestle with the practical and ethical issues of researching individual terrorists' experiences. However, analyses of the supply of content often suggest a degree of causality of influence over the individual that engages with it, which cannot be proven (von Behr et al. 2013).

This research has added to the small body of literature which bridges this gap, providing quantitative and qualitative analyses which simultaneously draw from previous research while using inductive methods of enquiry. This thesis demonstrates that it is possible to research this topic robustly without access to primary data; it remains difficult to conduct interview-based research with terrorists or to look at their private online records. However, there is a wealth of rich and granular data available from open sources. Ironically, the perception of the Internet as the primary venue for pathways towards terrorism increases the likelihood that online interactions will be mentioned in court documents or news sources, which has aided this research greatly. I hope that scholars of future research draw upon these methods of data collection to study the phenomenon further and that governments understand the value in making such sources available, either by making them accessible for anybody or sharing closed-source data such as police records with trusted researchers.

Bibliography

Academic

Al-Adnani, A.M., 2018. Indeed Your Lord is Ever Watchful. In D. Holbrook & C. Moore, [eds]. *Al Qaeda 2.0: A Critical Reader*. Oxford: Oxford University Press, pp. 153–165.

Al-Baghdadi, A.B., 2018. Friday Prayers and Sermon in the Grand Mosque of Mosul. In D. Holbrook & C. Moore, [eds]. *Al Qaeda 2.0: A Critical Reader*. Oxford: Oxford University Press, pp. 148–152.

Al-Rawi, A., 2016. Video games, terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence*, 30(4), pp. 740-760.

Alpert, M., 2017. By The Numbers: The United States of Refugees, *Smithsonian Magazine*, April. Available at: https://www.smithsonianmag.com/history/by-numbers-united-states-refugees-180962487/.

Alexander, A., 2019. A Plan for Preventing and Countering Terrorist and Extremist Exploitation of Information and Communication Technology in America. *George Washington University Program on Extremism*.

Alexander, A., 2016. Cruel Intentions: Female Jihadists in America. *George Washington University Program on Extremism*.

Alexander, A., 2017. Digital Decay? Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter, *George Washington University Program on Extremism*.

Alexander, A. & Braniff, W., 2018. Marginalizing Violent Extremism Online. *Lawfare Blog*, (January 21). Available at: https://www.lawfareblog.com/marginalizing-violent-extremism-online.

Alexander, A. & Clifford, B., 2019. Doxing and Defacements: Examining the Islamic State's Hacking Capabilities. *CTC Sentinel*, (April), pp.22–28.

Aly, A., 2017. Brothers, Believers, Brave Mujahideen: Focusing attention on the audience of violent jihadist preachers. *Studies in Conflict & Terrorism*, 40(1), pp.62–76.

Anti-Defamation League, 2014. *Homegrown Islamic Extremism in 2013*, New York. Available at: https://www.adl.org/news/article/homegrown-islamic-extremism-in-2013.

Archetti, C., 2015. Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age, *Perspectives on Terrorism*, 9(1), pp. 49–59.

Ardern, J., 2019. Christchurch Call to Eliminate Terrorist and Violent Extremist Online Content Adopted, New Zealand Government, May 16. Available at: https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted.

Azani, E., & Koblentz-Stenzler, L., 2019, Muslim Converts Who Turn to Global Jihad: Radicalization Characteristics and Countermeasures, *Studies in Conflict &*

Terrorism.

Azani, E. & Liv, N., 2018. Jihadists' Use of Virtual Currency, International Institiute for Counter-Terrorism, *International Institute for Counter Terrorism*.

Bakker, E., 2006. Jihadi Terrorists in Europe: Their characteristics and the circumstances in which they joined the jihad, *Clingendael Institute*.

Bakshy, E., Messing, S. and Adamic, L., 2015. Exposure to Ideologically Diverse News and Opinion on Facebook, *Science Express*, (May), pp. 1–5.

Bartlett, J., 2015. *The Dark Net*, London: Windmill Books.

Bartlett, J., 2017. *Radicals: Outsiders Changing the World*, London: William Heinemann.

Bartlett, J. & Miller, C., 2012. The Edge of Violence: Towards Telling the Difference Between Violent and Non-Violent Radicalization. *Terrorism and Political Violence*, 24(1), pp.1–21.

Basra, R., Neumann, P. & Brunner, C., 2016. Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus. *The International Centre for the Study of Radicalisation and Political Violence*.

Bastug, M.F., Douai, A. & Akca, D., 2018. Exploring the "Demand Side" of Online Radicalization: Evidence from the Canadian Context. *Studies in Conflict & Terrorism*.

Baugut, P. & Neumann, K., 2019. Online propaganda use During Islamist Radicalization. *Information Communication and Society*, pp.1–23.

von Behr, I. et al., 2013. Radicalisation in the Digital Era: The use of the internet in 15 cases of terrorism and extremism. *RAND Corporation*.

de Bie, J. and de Poot, C. Studying Police Files with Grounded Theory Methods to Understand Jihadist Networks, *Studies in Conflict & Terrorism*, 39 (7-8), pp. 580-601.

Behlendorf, B., Belur, J., and Kumar, S., 2016. Peering Through the Kaleidoscope: Variation and validity in data collection on terrorist attacks. *Studies in Conflict and Terrorism*, 39(7–8), pp. 641–667

Benedek, E. & Simon, N., 2020. The 2017 Manchester Bombing and the British-Libyan Jihadi Nexus, *CTC Sentinel,* Vol. 13(5), pp.1-12.

Benson, D.C., 2014. Why the Internet is not Increasing Terrorism. *Security Studies*, 23(2), pp.293–328.

Berger, J.M., 2017. Extremist Construction of Identity : How Escalating Demands for Legitimacy Shape and Define In- Group and Out-Group Dynamics. *International Centre for Counter-Terrorism*.

Berger, J.M. & Morgan, J., 2015. The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter. *The Brookings Project on U.S. Relations with the Islamic World: Analysis Paper*, March (20).

Berger, J.M. & Perez, H., 2016. The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters. *George Washington University: Program on Extremism*, (February).

Berkell, K., 2017. Risk Reduction in Terrorism Cases: Sentencing and the Post-Conviction Environment. *Journal for Deradicalization*, (13), pp.276–341.

Bermingham, A. et al., 2009. Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation. *Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining, ASONAM 2009*, pp.231–236.

Berrebi, C., 2007. Evidence about the Link Between Education, Poverty and Terrorism among Palestinians. *Peace Economics, Peace Science and Public Policy*, 13(1).

Biderman, A.D. & Reiss, A.J., 1967. On Exploring the "Dark Figure" of Crime. *The Annals of the American Academy of Political and Social Science*, 374(1), pp.1–15.

Bloom, M., Tiflati, H. & Horgan, J., 2017. Navigating ISIS's Preferred Platform: Telegram. *Terrorism and Political Violence.*

Borum, R., 2014. Psychological Vulnerabilities and Propensities for Involvement in Violent Extremism. *Behavioral Sciences & the Law*, 32(2), pp.286–305.

Borum, R., 2011a. Radicalization into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security*, 4(4), pp.7–36.

Borum, R., 2011b. Radicalization into Violent Extremism II: A review of Conceptual Models and Empirical Research. *Journal of Strategic Security (JSS)*, 4(4), pp.37–62.

Borum, R., 2011c. Rethinking Radicalization. *Journal of Strategic Security*, 4(4), pp.1–6.

Borum, R., 2017. The Etiology of Radicalization. In G. LaFree & J. D. Freilich, [eds.], *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 17–32.

Borum, R., 2003. Understanding the Terrorist Mindset. *FBI Law Enforcement Bulletin*, pp.7–10.

Botz-Bornstein, T., 2017. The "Futurist" Aesthetics of ISIS. *Journal of Aesthetics and Culture*, 9(1).

Bouhana, N. et al. 2016. Risk Analysis Framework, *Preventing, Interdicting and Mitigating Extremist events: Defending against lone actor extremism*.

Bouhana, N. et al., 2018. Background and Preparatory Behaviours of Right-Wing Extremist Lone Actors: A Comparative Study. *Perspectives on Terrorism*, 12(6).

Bouhana, N., 2019. The Moral Ecology of Extremism: A Systemic Perspective. *Commission for Countering Extremism*.

Brachman, J.M. & Levine, A.N., 2011. You Too Can Be Awlaki. *The Fletcher Forum of World Affairs*, 35(1), pp.25–46.

Broadbent, S. & Lobet-Maris, C., 2015. Towards a Grey Ecology, in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 111-124.

Bright, J., 2017. Explaining the emergence of echo chambers on social media: the role of ideology and extremism, *Oxford Internet Institute.*

Bryant, A., 2002. Re-grounding Grounded Theory. *Journal of Information Technology Theory and Application*, 4, pp. 25–42.

Bryman, A., 2006. Integrating quantitative and qualitative research: How is it done? *Qualitative Research*, 6(1), pp. 97-113.

Bryman, A., 2015. *Social Research Methods,* Oxford: Oxford University Press.

Bryson, R., 2017. *For Caliph and Country*, London: Tony Blair Institute for Global Change.

Burkell, J. et al., 2014. Facebook: Public Space, or Private Space? *Information, Communication & Society*, 17(8), pp.974–985.

Canetti, D. et al., 2013. Exposure to Political Violence and Political Extremism: A Stress-Based Process. *European Psychologist*, 18(4), pp.263–272.

Carter, J., Maher, S. & Neumann, P., 2014. #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks. *The International Centre for the Study of Radicalisation and Political Violence*.

Charmaz, K., 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. Sage Publications: Thousand Oaks, CA.

Chermak, S., Freilich, J. D., Parkin, W. S., and Lynch, J. P., 2012. American Terrorism and Extremist Crime Data Sources and Selectivity Bias: An investigation focusing on homicide events committed by far-right extremists. *Journal of Quantitative Criminology*, 28(1), 191–218.

Christmann, K., 2012. Preventing Religious Radicalisation and Violent Extremism: A Systematic Review of the Research Evidence. *Youth Justice Board*.

Clement, J., 2019, Internet Usage Worldwide – Statistics & Facts, *Statistica,* Available at: https://www.statista.com/topics/1145/internet-usage-worldwide/.

Clifford, B. & Powell, H., 2019. Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram. *George Washington University Program on Extremism*.

Cohen, J. N., 2018. Exploring Echo-Systems: How algorithms shape immersive media environments. *Journal of Media Literacy Education*. Vol. 10, pp. 139–151

Commission for Countering Extremism, 2019. Challenging Hateful Extremism.

Conway, M., 2012. From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu. *CTX: Combatting Terrorism Exchange*, 2(4), pp.12–22.

Conway, M., 2016a. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*, pp.1–22.

Conway, M., 2016b. Violent Extremism and Terrorism Online in 2016: The Year in Review. *Vox Pol*.

Conway, M. et al., 2017. Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts. *Vox Pol*.

Conway, M., 2018. Violent Extremism and Terrorism Online in 2018: The Year in Review. *Vox Pol*.

Conway, M., Parker, J., and Looney, S., 2017. Online Jihadi Instructional Content: The role of magazines, in: Conway et al. eds., *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam: IOS Press, pp. 182-193.

Conway, M. et al., 2018. Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts. *Studies in Conflict and Terrorism*, 42(1–2), pp.141–160.

Conway, M. & Courtney, M., 2017. Violent Extremism and Terrorism Online in 2017: The Year in Review. *Vox Pol*.

Cook, J. & Vale, G., 2018. From Daesh to "Diaspora": Tracing the Women and Minors of Islamic State. *International Centre for the Study of Radicalisation and Political Violence*.

Cook, J. & Vale, G., 2019. From Daesh to "Diaspora" II: The Challenges Posed by Women and Minors After the Fall of the Caliphate. *International Centre for the Study of Radicalisation and Political Violence*.

Corner, E., Bouhana, N. & Gill, P., 2018. The Multifinality of Vulnerability Indicators in Lone-Actor Terrorists. *Psychology, Crime and Law*, 25(2), pp.111-132.

Corner, E. & Gill, P., 2019. Psychological Distress, Terrorist Involvement and Disengagement from Terrorism: A Sequence Analysis Approach. *Journal of Quantitative Criminology*.

Corner, E. & Gill, P., 2018. The Nascent Empirical Literature on Psychopathology and Terrorism. *World Psychiatry*, (June), pp.147–148.

Corner, E., Gill, P. & Mason, O., 2016. Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence. *Studies in Conflict & Terrorism*, 39(6), pp.560–568.

Cottee, S. & Cunliffe, J., 2018. Watching ISIS: How Young Adults Engage with Official English-Language ISIS Videos. *Studies in Conflict & Terrorism*.

Council of the European Union, nd, EU Fight Against Terrorism, Available at: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/#

Council of the European Union, 2014, Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism, Available at:

http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf.

Counter Extremism Project, 2018. Ok Google, Show Me Extremism: Analysis of YouTube's Extremist Video Takedown Policy and Counter-Narrative Program. Available at: https://www.counterextremism.com/ok-google.

Counter Extremism Project, nd. Terrorist and Extremist Database. Available at: https://www.counterextremism.com/extremists.

Crenshaw, M., 2007. The Debate over "New" vs "Old" Terrorism. *Presented at the Annual Meeting of the American Political Science Association, Chicago*.

Cruz, E., D'Alessio, S.J., Stolzenberg, L., 2018. The Labor Market and Terrorism, *Studies in Conflict & Terrorism*.

Dauber, C.E. et al., 2019. Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. *Perspectives on Terrorism*, 13(3), pp.17–31.

Desmarais, S. L. et al. The state of Scientific Knowledge Regarding Factors Associated with Terrorism, *Journal of Threat Assessment and Management*, 4(4), pp. 180-209

Dey, I., 2011. Grounding Categories. In A. Bryant & K. Charmaz, [eds.], *The SAGE Handbook of Grounded Theory*. London: Sage Publications, pp. 166–190.

Doosje, B. et al., 2016. Terrorism, Radicalization and De-radicalization. *Current Opinion in Psychology*, 11, pp.79–84.

Droogan, J. & Peattie, S., 2016. Reading jihad: Mapping the shifting themes of Inspire magazine. *Terrorism and Political Violence*, 30(4) pp.684–717.

Ducol, B., 2015. A radical sociability: In defense of an online/offline multidimensional approach to radicalization, in Bouchard, M. (ed.) *Social Networks, Terrorism, and Counter-Terrorism: Radical and Connected*. London: Routledge, pp. 82–104.

Ducol, B. et al., 2016. Assessment of the state of knowledge: Connections between research on the social psychology of the Internet and violent extremism, *Canadian Network for Research on Terrorism, Security and Society*.

Dugas, M. & Kruglanski, A., 2014. The Quest for Significance Model of Radicalization: Implications for the Mangement of Terrorist Detainees. *Behavioral Sciences & the Law*, 32, pp.423–439.

Durodie, B. & Ng, S.C., 2008. Is Internet Radicalization Possible ? *RSIS Commentaries*.

El-Said, H. & Barrett, R., 2017. Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria. *United Nations Office of Counter-Terrorism*.

Ess, C. 2015. The Onlife Manifesto: Philosophical Backgrounds, Media Usages, and the Futures of Democracy and Equality, in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 89-110.

EU Parliament, 2019. Terrorist Content Online Should be Removed Within One Hour, Says EP, Press Release, April 17. Available at:

https://www.europarl.europa.eu/news/en/press-room/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-says-ep.

Europol, 2014. *TE SAT: European Union Terrorism Situation and Trend Report*, The Hague

Europol, 2017. *TE SAT: European Union Terrorism Situation and Trend Report*, The Hague.

Europol, 2018. *TE SAT: European Union Terrorism Situation and Trend Report*, The Hague.

Europol, 2019a. *TE SAT: European Union Terrorism Situation and Trend Report*, The Hague.

Europol, 2019b. Women in Islamic State Propaganda: Roles and Incentives. *Europol Specialist Reporting*. The Hague.

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

Federal Bureau of Investigation, nd, What We Investigate – Terrorism, Available at: https://www.fbi.gov/investigate/terrorism.

Federal Deposit Insurance Corporation, 2018. Share of U.S. Households without a Bank Account Continues to Drop, October 23. Available at: https://www.fdic.gov/news/news/press/2018/pr18077.html.

Federico, C.M., Hunt, C. V. & Fisher, E.L., 2013. Uncertainty and Status-Based Asymmetries in the Distinction Between the "Good" Us and the "Bad" Them: Evidence That Group Status Strengthens the Relationship Between the Need for Cognitive Closure and Extremity in Intergroup Differentiation. *Journal of Social Issues*, 69(3), pp.473–494.

Field, A., 2018. *Discovering Statistics Using IBM SPSS Statistics* 5th ed., London: Sage Publications.

Fisher, A., 2015. Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence. *Perspectives on Terrorism*, 9(3), pp.3–20.

Fisher, A., Prucha, N. & Winterbotham, E., 2019. Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability. *Global Research Network on Terrorism and Technology*, (6).

Fletcher, G., 2006. The Indefinable Concept of Terrorism, *Journal of International Criminal Justice*, 4(5), pp. 894-911.

Floridi, L. 2007. 'A look into the future impact of ICT on our lives', *Information Society*, 23(1), pp. 59–64.

Floridi, L. 2015. Introduction, in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 1-7.

Floridi, L., et al. 2015. The Onlife Manifesto. in: Floridi, L. [Ed.] *The Onlife Manifesto:*

Being Human in a Hyperconnected Era, London: SpringerOpen, pp. 7-16.

Fodeman, A., Snook, D., & Horgan, J., 2020. Picking Up and Defending the Faith: Activism and Radicalism Among Muslim Converts in the United States, *Political Psychology*.

Frenet, R. & Dow, M., 2018. One to One Online Interventions: A pilot CVE methodology, *Instutite for Strategic Dialogue*.

Friis, S.M., 2015. "Beyond Anything we Have Ever Seen": Beheading videos and the visibility of violence in the war against ISIS. *International Affairs*, 91(4), pp.725–746.

Frischlich, L. et al., 2015. Dying the Right-way? Interest in and perceived persuasiveness of parochial extremist propaganda increases after mortality salience. *Frontiers in Psychology*, 6(August), pp.1–11.

Gallie, W. B., 1955. Essentially Contested Concepts, *Proceedings of the Aristotelian Society*, 56, pp. 167-198.

Ganascia, J. 2015. Views and Examples on Hyper-Connectivity. in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 65-88.

Ganor, B., 2002. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? *Police Practice and Research*, 29(3), pp.123–133.

Gartenstein-Ross, D. & Grossman, L., 2009. *Homegrown terrorists in the US and the UK: An Empirical Examination of the Radicalization Process*, FDD Press: Washington, D.C.

Gendron, A., 2017. The Call to Jihad: Charismatic Preachers and the Internet. *Studies in Conflict & Terrorism*, 40(1), pp.44–61.

Gentzkow, M. and Shapiro, J. M., 2011. Ideological Segregation Online and Offline, *Quarterly Journal of Economics*, 126(4), pp. 1799–1839.

Gill, P., 2016. Online Behaviours of Convicted Terrorists. *Vox Pol*.

Gill, P. et al., 2017. Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes. *Criminology and Public Policy*, 16(1), pp.99–117.

Gill, P. et al., 2015. What are the Roles of the Internet in Terrorism? *Vox Pol*..

Gill, P. & Corner, E., 2013. Disaggregating Terrorist Offenders: Implications for Research and Practice. *Criminology and Public Policy*, 12(1), pp.93–101.

Gill, P. & Corner, E., 2015. Lone Actor Terrorist Use of the Internet and Behavioural Correlates. In L. Jarvis, S. Macdonald, & T. M. Chen, [eds.], *Terrorism Online: Politics Law and Technology*. Abingdon, Oxon: Routledge, pp. 35–53.

Gill, P. & Corner, E., 2017. There and Back Again There and Back Again: The Study of Mental Disorder and Terrorist Involvement. *American Psychologist*, pp.1–35.

Gill, P., Horgan, J. & Deckert, P., 2014. Bombing Alone: Tracing the Motivations and

Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences*, 59(2), pp.425–435.

Githens-Mazer, J. & Lambert, R., 2010. Why Conventional Wisdom on Radicalization Fails: The persistence of a failed discourse. *International Affairs*, 86(4), pp.889–901.

Glaser, B.G., 2001. *The Grounded Theory Perspective: Conceptualization Contrasted with Description*, Mill Valley, CA: Sociology Press.

Glaser, B.G., 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, Mill Valley, CA: The Sociology Press.

Glaser, B.G. & Strauss, A.L., 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, New Brunswick, NJ: AldineTransaction.

Glaser, B.G., 2007. Doing Formal Theory, in: Bryant, A. and Charmaz, K. [Eds.], *The SAGE Handbook of Grounded Theory*, Sage Publications: London.

Glazzard, A., 2017. Losing the Plot: Narrative, Counter-Narrative and Violent Extremism, *International Centre for Counter-Terrorism*.

Global Internet Forum to Counter Terroism, nd. Global Internet Forum to Counter Terrorism: Evolving an Institution. Available at: https://gifct.org/about/.

Global Internet Forum to Counter Terrorism, 2019. Joint Statement in Support of Christchurch Call. Available at: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2019/05/Christchurch-Call-and-Nine-Steps.pdf.

Golden, S.H. & Bass, E.B., 2013. Validity of Meta-Analysis in Diabetes: Meta-analysis is an Indispensable Tool in Evidence Synthesis. *Diabetes Care*, 36(10), pp.3368–3373.

Gomez-Uribe, C.A. & Hunt, N., 2015. The Netflix Recommender System: Algorithms, business value, and innovation. *ACM Transactions on Management Information Systems*, 6(4).

Google, 2016. The Redirect Method. Available at: https://redirectmethod.org/.

Greenberg, K.J. & Weiner, S., 2017. The American Exception: Terrorism Prosecution In the United States - The ISIS Cases- March 2014 - August 2017, *Center on National Security at Fordham Law*.

Greene, J. C. 2007. *Mixed Methods in Social Inquiry*. San Francisco, CA: Jossey-Bass.

Grinnell, D. et al., 2018. Who Disseminates Rumiyah? Examining the relative influence of sympathiser and non-sympathiser Twitter users, *2nd European Counter Terrorism Centre (ECTC) Advisory Group*, Europol, The Hague.

Grinnell, D., Macdonald, S. & Mair, D., 2017. The Response of, and on ,Twitter to the Release of Dabiq Issue 15. *European Counter Terrorism Centre (ECTC) Advisory Group*, Europol, The Hague.

Grundlingh, L., 2018. Memes as Speech Acts. *Social Semiotics*, 28(2), pp.147–168.

Guhl, J., 2018. Why Beliefs Always Matter, But Rarely Help us Predict Jihadist Violence.

The role of cognitive extremism as a precursor for violent extremism, *Journal for Deradicalization*, 14, pp.192–217.

Gündüz, U., 2017. The Effect of Social Media on Identity Construction. *Mediterranean Journal of Social Sciences*, 8(5), pp.85–92.

Hafez, M.M. & Mullins, C., 2015. The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism. *Studies in Conflict & Terrorism*, 38(11), pp. 958-975.

Halpern, D. & Gibbs, J., 2013. Social Media as a Catalyst for Online Deliberation? Exploring the affordances of Facebook and YouTube for political expression. *Computers in Human Behavior*, 29(3), pp.1159–1168.

Halverson, J.R. & Way, A.K., 2012. The Curious Case of Colleen LaRose: Social margins, new media, and online radicalization. *Media, War & Conflict*, 5(2), pp.139–153.

Hardy, K. & Williams, G., 2011. What is Terrorism? Assessing Domestic Legal Definitions. *UCLA Journal of International Law and Foreign Affairs*, 16, pp.77–162.

Harris, K., Gringart, E., and Deirdre, D., Understanding the role of social groups in radicalisation, *7th Australian Security and Intelligence Conference, Edith Cowan University, Perth, Western Australia*, 1-3 December, 2014

Hegghammer, T., 2014. Interpersonal Trust on Jihadi Internet Forums, *Norwegian Defence Research Establishment*.

Hegghammer, T., 2013. Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting. *American Political Science Review*, 107(1), pp.1–15.

Hegghammer, T. & Nesser, P., 2015. Assessing the Islamic State's Commitment to Attacking the West. *Prespectives on Terrorism*, 9(4), pp.14–30.

Helfstein, S., 2012. *Edges of Radicalization: Ideas, Individuals and Networks in Violent Extremism*, U.S. Military Academy, Combating Terrorism Center, West Point, NY.

HM Government, 2017, UK and France Announce Joint Campaign to Tackle Online Radicalisation, Available at: https://www.gov.uk/government/news/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation.

HM Government, 2019. *Online Harms White Paper*, London: The Stationary Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Hogg, M.A. & Adelman, J., 2013. Uncertainty-Identity Theory: Extreme Groups, Radical Behavior, and Authoritarian Leadership. *Journal of Social Issues*, 69(3), pp.436–454.

Hogg, M.A., Kruglanski, A. & van den Bos, K., 2013. Uncertainty and the Roots of Extremism. *Journal of Social Issues*, 69(3), pp.407–418.

Holbrook, D. & Taylor, M. 2017. Terrorism as Process Narratives: A study of pre-arrest

media usage and the emergence of pathways to engagement. *Terrorism and Political Violence*, 31(6), pp. 1307-1326.

Holbrook, D., 2019. The Terrorism Information Environment: Analysing Terrorists' Selection of Ideological and Facilitative Media. *Terrorism and Political Violence*, pp.1–23.

Holbrook, D., 2017. What Types of Media Do Terrorists Collect? *International Centre for Counter-Terrorism*.

Holt, T.J. et al., 2015. Political Radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, 8(2), pp.107–120.

Holt, T.J., Freilich, J.D. & Chermak, S., 2016. Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures. *Deviant Behavior*, pp.1–15.

HM Home Office, 2018. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf.

HM Home Office, 2015. *Revised Prevent Duty Guidance for England and Wales*, London. Available at: www.gov.uk/government/publications/prevent guidance.

HM Parliament, 2016. *Radicalisation: The Counternarrative and Identifying the Tipping Point*, The Stationary Office: London.

Horgan, J. et al., 2016. Actions Speak Louder than Words: A Behavioral Analysis of 183 Individuals Convicted for Terrorist Offenses in the United States from 1995 to 2012. *Journal of Forensic Sciences*, 61(5), pp.1228–1237.

Horgan, J., 2008. From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism. *The Annals of the American Academy of Political and Social Science*, 618(1), pp.80–94.

Hoyle, C., Bradford, A. & Frenet, R., 2015. Becoming Mulan? Female Western Migrants to ISIS. *Institute for Strategic Dialogue*.

Huey, L., 2015. This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming. *Journal of Terrorism Research*, 6(2), pp.1–16.

Huey, L., Inch, R. & Peladeau, H., 2017. "@ me if you need shoutout": Exploring Women's Roles in Islamic State Twitter Networks. *Studies in Conflict and Terrorism*, 42(5), pp. 445-463.

Huey, L. & Witmer, E., 2016. # IS _ Fangirl : Exploring a New Role for Women in Terrorism. *Journal of Terrorism Research*, 7(1), pp.1–10.

Hughes, S. and Clifford, B., First He Became an American, Then He Joined ISIS, *The Atlantic*, May 25, 2017. Available at: https://www.theatlantic.com/international/archive/2017/05/first-he-became-an-

americanthen-he-joined-isis/527622/.

Hughes, S. & Meleagrou-Hitchens, A., 2017. The Threat to the United States from the Islamic State's Virtual Entrepreneurs. *CTC Sentinel*, 10(3), pp.1–9.

Hughes, S. Meleagrou-Hitchens, A., and Clifford, B., A New American Leader Rises in ISIS, *The Atlantic*, January 13, 2018. Available at: https://www.theatlantic.com/international/archive/2018/01/isis-america-hoxha/550508/.

Hughes, S. The Only Islamic State-Funded Plot in the US: The Curious Case of Mohamed Elshinawy, *Lawfare Blog*, March 7 2018. Available at: https://www.lawfareblog.com/only-islamic-state-funded-plot-us-curious-case-mohamed-elshinawy.

Human Rights Watch, 2014. *Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions*. Columbia Law School.

Hunter, R. & Heinke, D., 2011. Radicalization of Islamist Terrorists in the Western World. *FBI Law Enforcement Bulletin*, September. Available at: https://leb.fbi.gov/2011/september/perspective-radicalization-of-islamist-terrorists-in-the-western-world.

Hussain, G. & Saltman, E.M., 2014. Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it. *Quilliam Foundation.*

Ingram, H., 2014. Three Traits of the Islamic State's Information Warfare. *RUSI Journal*, 159(6), pp.4–11.

Ingram, H., 2015. The strategic logic of Islamic State information operations. *Australian Journal of International Affairs*, 69(6), pp.729–752.

Ingram, H., 2016a. An analysis of Islamic State's Dabiq magazine. *Australian Journal of Political Science*, 51(3), pp.458–477.

Ingram, H., 2016b. Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility & Behavioural Change. *International Centre for Counter-Terrorism*.

Ingram, H., 2018. Islamic State's English-language Magazines , 2014-2017: Trends & implications for CT-CVE strategic communications. *International Centre for Counter-Terrorism*.

Institute for Strategic Dialogue, 2011. *Radicalisation: The Role of the Internet*.

Internet World Statistics, 2019. Internet Usage Statistics: The Internet Big Picture - World Internet Users and 2019 Population Stats. Available at: https://www.internetworldstats.com/stats.htm.

Investigative Project on Terrorism, nd. Cases. Available at: https://www.investigativeproject.org/cases.php.

Janis, I., 1971. Groupthink, *Psychology Today*, 5(6), pp. 84–90.

Jackson, R., 2012. The Study of Terrorism 10 Years after 9/11: Successes, issues,

challenges, *Uluslararası İlişkiler Dergisi*, 8(32); pp.1-16.

Jasko, K., LaFree, G. & Kruglanski, A., 2017. Quest for Significance and Violent Extremism: The Case of Domestic Radicalization. *Political Psychology*, 38(5), pp.815–831.

Jensen, M., James, P., et al., 2018. The Use of Social Media by United States Extremists. *National Consortium for the Study of Terrorism and Responses to Terrorism*.

Jensen, M., Atwell Seate, A. & James, P.A., 2018. Radicalization to Violence: A Pathway Approach to Studying Extremism. *Terrorism and Political Violence*.

Johansson, A., 2017. ISIS-chan – the Meanings of the Manga girl in Image Warfare Against the Islamic State. *Critical Studies on Terrorism*, 11(1), 1-25.

Jones, S. et al., 2017. Rolling Back the Islamic State. *RAND Corporation*.

Jurgenson, N., 2012. When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution, *Future Internet*, 4(1), pp. 83–91.

Kahneman, D., 2012. *Thinking, Fast and Slow*, London: Penguin.

Keatinge, T. & Keen, F., 2017. Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance? *Royal United Services Institute for Defence and Security Studies*.

Kellner, D., 2007. The Media in and After 9/11, *International Journal of Communication Book Review*, 1, pp.123-142.

Kemp, S., 2019. Digital 2019: The United States of America, *Data Portal*, January 31. Available at: https://datareportal.com/reports/digital-2019-united-states-of-america.

Ki-moon, B., More 'Concrete Steps' Needed by Nations to Counter Terrorism, Ban Tells Security Council, *UN News*, Available at: https://news.un.org/en/story/2016/04/526712-more-concrete-steps-needed-nations-counter-terrorism-ban-tells-security-council.

King, M. & Taylor, D.M., 2011. The Radicalization of Homegrown Jihadists: A Review of Theoretical Models and Social Psychological Evidence. *Terrorism and Political Violence*, 23(4), pp.602–622.

Klausen, J., 2016a. A Behavioral Study of the Radicalization Trajectories of American "Homegrown" Al Qaeda-Inspired Terrorist Offenders.

Klausen, J. et al., 2018. Radicalization Trajectories: An Evidence-Based Computational Approach to Dynamic Risk Assessment of "Homegrown" Jihadists. *Studies in Conflict & Terrorism*.

Klausen, J., 2016b. The Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990-2015, *National Criminal Justice Reference Service*.

Klausen, J. et al., 2016. Towards a Behavioral Model of "Homegrown" Radicalization

Trajectories. *Studies in Conflict & Terrorism*, 39(1), pp.67–83.

Klausen, J., 2015. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), pp.1–22.

Kleinmann, S.M., 2012, Radicalization of Homegrown Sunni Militants in the United States: Comparing converts and non-converts, *Studies in Conflict & Terrorism*, 35(4), pp.278-297.

Kock, N., & Lynn, G., 2012. Lateral Collinearity and Misleading Results in Variance-based SEM: An illustration and recommendations, *Journal of the Association for Information Systems*, 13(7), pp. 546-580

Koehler, D., 2014. The Radical Online: Individual Radicalization Processes and the Role of the Internet. *Journal for Deradicalization*, (1), pp.116–134.

Krasodomski-Jones, A., 2017. *Talking To Ourselves? Political Debate Online and the Echo Chamber Effect*. London.

Kruglanski, A. et al., 2014. The Psychology of Radicalization and Deradicalization: How significance quest impacts violent extremism. *Political Psychology*, 35, pp.69–93.

Lafree, G. et al., 2018. Correlates of Violent Political Extremism in the United States. *Criminology*, 56(2), pp.233–268.

LaFree, G., 2017. Terrorism and the Internet. *Criminology & Public Policy*, 16(1), pp.1–6.

Lafree, G. & James, P., 2014. Profiles of Individual Radicalization in the United States (PIRUS) An Empirical Assessment of Domestic Radicalization. *National Consortium for the Study of Terrorism and Responses to Terrorism*.

Lakomy, M., 2017a. Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace. *Perspectives on Terrorism*, 11(3), pp.40–53.

Lakomy, M., 2017b. Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. *Studies in Conflict & Terrorism*, 42(4), pp.383-406.

Lange, P. G. 2007. Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication*, Vol 13(1).

Larson, M. G. 2008. Analysis of Variance, *Circulation*, 117(1), pp. 115-121.

Lee, D. 2017. Message Encryption a Problem – Rudd, *BBC News*, August 1. Available at: https://www.bbc.co.uk/news/technology-40788180.

Lehane, O., 2017. *Mining the Personal to Carve a Space of One's Own: A Grounded Theory Study of Grassroots Countering Violent Extremism Practitioners*, Doctoral Thesis, Dublin City University.

Leiner, B.M. et al., 2009. A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), pp.22–31.

Leistedt, S.J., 2016. On the Radicalization Process. *Journal of Forensic Sciences*, 61(6), pp.1588–1591.

Lemieux, A.F. et al., 2014. Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model. *Terrorism and Political Violence*, 26(2), pp.354–371.

Levin, B., 2015. The Original Web of Hate: Revolution Muslim and American Homegrown Extremists. *American Behavioral Scientist*, 59(12), pp.1609–1630.

Lewis, G.J., Graham, G. & Hardaker, G., 2005. Evaluating the Impact of the Internet on Barriers to Entry in the Music Industry. *Supply Chain Management*, 10(5), pp.349–356.

Liem, M. et al., 2017. European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis. *Homicide Studies*, 22(1), pp. 45-69.

Lorenzo-Dus, N., Kinzel, A. & Walker, L., 2018. Representing the West and "Non-believers " in the Online Jihadist Magazines Dabiq and Inspire. *Critical Studies on Terrorism*.

Lorenzo-Dus, N. & Macdonald, S., 2018. Othering the West in the Online Jihadist Propaganda Magazines Inspire and Dabiq. *Journal of Language Aggression and Conflict*, 6(1), pp.79–188.

Lygre, R.B. et al., 2011. Terrorism as a Process: A critical review of Moghaddam's "Staircase to Terrorism." *Scandinavian Journal of Psychology*, 52(6), pp.609–616.

Macdonald, S., 2016. Terrorist Narratives & Communicative Devices: Findings. In: Zeiger, S. ed. *Expanding Research on Countering Violent Extremism*, Hedayah Centre: Abu Dhabi.

Macdonald, S., Grinnell, D., et al., 2019. A Study of Outlinks Contained in Tweets Mentioning Rumiyah. *Global Research Network on Terrorism and Technology*, (2).

Macdonald, S., Correia, S.G. & Watkin, A.-L., 2019. Regulating terrorist content on social media: Automation and the rule of law. *International Journal of Law in Context*, 15(2), pp.183–197.

Macdonald, S. & Lorenzo-Dus, N., 2019. Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines. *Studies in Conflict & Terrorism*.

Macdonald, S. & Mair, D., 2015. Terrorism Online: A New Strategic Environment. In T. M. Chen, L. Jarvis, & S. Macdonald, eds. *Terrorism Online: Politics Law and Technology*. Abingdon, Oxon: Routledge, pp. 1–26.

Macdonald, S. & Whittaker, J., 2019. Online Radicalization: Contested Terms and Conceptual Clarity. In *Online Terrorist Propaganda, Recruitment, and Radicalisation*. Boca Raton, FL: CRC Press, pp. 33–46.

Mahmood, S. 2019. Negating Stereotypes: Women, Gender, and Terrorism in Indonesia and Pakistan, in: Alexander, A., [Ed.], Perspectives on the Future of Women, Gender, & Violent Extremism, George Washington University Program on Extremism, 2019, pp.11-21.

Manrique, P. et al., 2016. Women's connectivity in Extreme Networks. *Science Advances*,

2(6), pp.1–7.

Mccauley, C. & Moskalenko, S., 2010. Individual and Group Mechanisms of Radicalization. In L. Fenstermacher et al., [eds.], *Protecting the Homeland from International and Domestic Threats*. Boston, MA: NSI, Inc, pp. 82–31.

Mccauley, C. & Moskalenko, S., 2017. Understanding Political Radicalization: The Two-Pyramids Model. *American Psychologist*, 72(3), pp.205–216.

McCauley, C. & Moskalenko, S., 2008. Mechanisms of Political Radicalization: Pathways toward terrorism. *Terrorism and Political Violence*, 20(3), pp.415–433.

McKenna, K. Y. and Bargh, J. A., 1998. Coming out in the age of the Internet: Identity "demar- ginalization" through virtual group participation. *Journal of Personality and Social Psychology*, 75(3): 681–694.

Meleagrou-Hitchens, A., 2011. As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad. *International Centre for the Study of Radicalisation and Political Violence*.

Meleagrou-Hitchens, A., Hughes, S. & Clifford, B., 2018. The Travelers: American Jihadists in Syria and Iraq. *George Washington University Program on Extremism*.

Meleagrou-Hitchens, A. & Kaderbhai, N., 2017. Research Perspectives on Online Radicalisation: A Literature Review, 2006-2016. *Vox Pol*.

Meserole, C. & Byman, D., 2019. Terrorist Definitions and Designations Lists Key Findings and Recommendations. *Global Research Network on Terrorism and Technology*, (7).

Moghaddam, F.M., 2005. The Staircase to Terrorism: A Psychological Exploration. *American Psychologist*, 60(2), pp.161–169.

Mohamed, B., & Scuipac, E., 2018. The Share of Americans Who Leave Islam is Offset by Those Who Become Muslim, *Pew Research Center*, January 26. Available at: https://www.pewresearch.org/fact-tank/2018/01/26/the-share-of-americans-who-leave-islam-is-offset-by-those-who-become-muslim/.

Morse, J.M., 2011. Sampling in Grounded Theory. In A. Bryant & K. Charmaz, [eds.] *The SAGE Handbook of Grounded Theory*. London: Sage Publications, pp. 229–243.

Mruck, K. and Mey, G., 2019. Grounded Theory Methodology and Self-Reflexivity in the Qualitative Research Process, in: Charmaz, K. and Bryant, T. [Eds.] *The SAGE Handbook of Current Developments in Grounded Theory*, pp. 470-496.

Munger, K, and Phillips, J., 2020, Right-Wing YouTube: A Supply and Demand Perspective, *International Journal of Press/Politics*.

Nanninga, P., 2019. Branding a Caliphate in Decline: The Islamic State's Video Output (2015-2018). *International Centre for Counter-Terrorism*.

National Alliance on Mental Illness, nd. Mental Health By The Numbers. Available at: https://www.nami.org/learn-more/mental-health-by-the-numbers.

Neo, L. S., 2016. An Internet-Mediated Pathway for Online Radicalisation: RECRO, in Khader, M. (ed.) *Combating Volent Extremism and Radicalization in the Digital Era*. Hershey, PA: Information Science Reference, pp. 197–224.

Nesser, P., 2012. Research Note: single actor terrorism: scope, characteristics and explanations. *Perspectives on Terrorism*, 18(6), pp. 61–72.

Nesser, P., Stenersen, A. & Oftedal, E., 2016. Jihadi terrorism in Europe: The IS-effect. *Perspectives on Terrorism*, 10(6), pp.3–24.

Neumann, P., 2013a. Options and Strategies for Countering Online Radicalization in the United States. *Studies in Conflict & Terrorism*, 36(6), pp.431–459.

Neumann, P., 2013b. The Trouble with Radicalization. *International Affairs*, 89(4), pp.873–893.

Nissenbaum, A. & Shifman, L., 2017. Internet Memes as Contested Cultural Capital: The case of 4chan's /b/ board. *New Media and Society*, 19(4), pp.483–501.

Novenario, C.M.I., 2016. Differentiating Al Qaeda and the Islamic State Through Strategies Publicized in Jihadist Magazines. *Studies in Conflict & Terrorism*, 39(11), pp.953–967.

Nvivo, nd a. About Automated Insights. Available at: http://help-nv11.qsrinternational.com/desktop/concepts/about_automated_insights.htm.

Nvivo, nd b. Run a Word Frequency Query. Available at: http://help-nv11.qsrinternational.com/desktop/procedures/run_a_word_frequency_query.htm.

O'Callaghan, D. et al., 2015. Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems. *Social Science Computer Review*, 33(4), pp.459–478.

O'Hara, K. and Stevens, D. (2015) 'Echo Chambers and Online Radicalism: Assessing the Internet's Complicity in Violent Extremism', *Policy and Internet*, 7(4), pp. 401–422.

Pantano, E. et al., 2016. *Internet Retailing and Future Perspectives*, Second Edition, London: Routledge.

Pattie, C. and Johnston, R., 2016. 'Talking with one voice? Conversation networks and political polarisation', *The British Journal of Politics and International Relations*, 18(2), pp. 482–497.

Pauwels, L. and Schils, N., 2016. Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives. *Terrorism and Political Violence*, 28(1); pp. 1-29.

Pearson, E., 2017. Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media. *Studies in Conflict and Terrorism*. 41(11), pp.850-874.

Pearson, E., 2016. The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad. *Policy and Internet*, 8(1), pp.5–33.

Pearson, E. & Winterbotham, E., 2017. Women, Gender and Daesh Radicalisation: A milieu approach. *RUSI Journal*, 162(3), pp.60–72.

Pearson, E., 2019, How Gender Matters in Violent Extremism & Efforts to Counter It, in: Atamuradova, F. et at. Eds., *Lessons from P/CVE Research: Innovative Methods, Challenges, and Good Practices*, Hedayah: Abu Dhabi, pp. 95-116.

Peddell, D., Eyre, M., McManus, M, Bonworth, J., 2016. Influences and Vulnerabilities in Radicalised Lone-actor Terrorists: UK practitioner perspectives, *International Journal of Police Science & Management*, 18(2), pp.63-76.

Pelletier, I.R. et al., 2016. Why ISIS's Message Resonates: Leveraging Islam, sociopolitical catalysts, and adaptive messaging. *Studies in Conflict and Terrorism*, 39(10), pp.871–899.

Pettinger, T., 2015. What is the Impact of Foreign Military Intervention on Radicalization? *Journal for Deradicalization*, (5), pp.92–119.

Pew Research Centre, 2017a. Demographic Portrait of Muslim Americans, July 26. Available at: https://www.pewforum.org/2017/07/26/demographic-portrait-of-muslim-americans/.

Pew Research Center, 2017b. Internet Use by Age, January 11. Available at: https://www.pewresearch.org/internet/chart/internet-use-by-age/.

Pew Research Center, 2018. Social Media Use in 2018. March 1. Available at: https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/.

Pew Research Center, 2019. Internet/Broadband Fact Sheet, June 12. Available at: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

Phillips, B. J., 2015, What Is a Terrorist Group? Conceptual Issues and Empirical Implications, *Terrorism and Political Violence*, 27(2), pp. 225-242.

Piazza, J.A., 2008. Incubators of Terror: Do failed and failing states promote transnational terrorism? *International Studies Quarterly*, 52(3), pp.469–488.

Piazza, J.A., 2011. Poverty, Minority Economic Discrimination, and Domestic terrorism. *Journal of Peace Research*, 48(3), pp.339–353.

Piazza, J.A., 2006. Rooted in poverty?: Terrorism, Poor Economic Development, and Social Cleavages. *Terrorism and Political Violence*, 18(1), pp.159–177.

Picart, C., 2015. "Jihad Cool/Jihad Chic": The Roles of the Internet and Imagined Relations in the Self-Radicalization of Colleen LaRose (Jihad Jane). *Societies*, 5(2), pp.354–383.

Polat, R.K., 2005. The Internet and Political Participation: Exploring the explanatory Links. *European Journal of Communication*, 20(4), pp.435–459.

Poole, E., 2016. Constructing "British Values" Within a Radicalisation Narrative: The reporting of the Trojan Horse affair. *Journalism Studies*.

Post, J., 2015. Terrorism and Right-wing Extremism: The changing face of terrorism and

political violence in the 21st century: The virtual community of hatred. *International Journal of Group Psychotherapy*, 65(2), pp.242–271.

Post, J., McGinnis, C. & Moody, K., 2014. The Changing Face of Terrorism in the 21st Century: The Communications Revolution and the Virtual Community of Hatred. *Behavioral Sciences & the Law*, 32(2), pp.306–336.

Powers, S.M., 2014. Conceptualizing Radicalization in a Market for Loyalties. *Media, War & Conflict*, 7(2), pp.233–249.

Precht, T., 2007. Home Grown Terrorism and Islamist Radicalisation in Europe - from Conversion to Terrorism. *Danish Ministry of Justice*.

Prensky, M., 2001. Digital Natives, Digital Immigrants. *On the Horizon*, 9(5), pp.1–6.

Program on Extremism, 2019a. ISIS in America: The Cases. *George Washington University*. Available at: https://extremism.gwu.edu/cases.

Program on Extremism, 2019b. The Travelers. *George Washington University*. Available at: https://extremism.gwu.edu/travelers.

Prucha, N., 2016. IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram. *Perspectives on Terrorism*, 10(6), pp.48–58.

Prucha, N. & Fisher, A., 2013. Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda. *CTC Sentinel*, 6(6), pp.19–23.

Pruyt, E. & Kwakkel, J., 2014. Radicalization Under Deep Uncertainty: a Multi-model Exploration of Activism, Extremism, and Terrorism. *Supporting Dynamics Review*, 30(1), pp.1–28.

Pyszczynski, T. et al., 2006. Mortality Salience, Martyrdom, and Military Might: The Great Satan Versus the Axis of Evil. *Personality and Social Psychology Bulletin*, 32(4), pp.525–537.

Raban, O., 2018. Observations on the First Amendment and the War on Terror. *Tulsa Law Review*, 53(2), pp.141–157.

Ralph, N., Birks, M. & Chapman, Y., 2015. The Methodological Dynamism of Grounded Theory. *International Journal of Qualitative Methods*, 14(4), pp.1–6.

Ramsay, G., 2015. Why Terrorism Can, but Should not be Defined. *Critical Studies on Terrorism*, 8(2), pp.211–228.

Ranganatham, P., Pramesh, C.S. & Aggarwal, R., 2017. Common Pitfalls in Statistical Analysis: Logistic Regression. *Perspect Clin Res*, 8, pp.148–151.

Reed, A. et al., 2019. Radical Filter Bubbles: Social Media Personalisation Algorithms and Extremist Content. *Global Research Network on Terrorism and Technology*, (8).

Reed, A. & Ingram, H., 2019. A Practical Guide to the First Rule of CT-CVE Messaging. 2nd European Counter-Terrorism Centre (ECTC) Advisory Group Conference.

Reed, A. & Ingram, H., 2017. Exploring the Role of Instructional Material in AQAP's

Inspire and ISIS' Rumiyah. *1st European Counter Terrorism Centre (ECTC) Conference on Online Terrorist Propaganda*.

Reeve, Z., 2019. Engaging with Online Extremist Material: Experimental Evidence. *Terrorism and Political Violence*.

Rey, P. J. and Boesel, W. E., 2014. 'The web, digital prostheses, and augmented subjectivity', *Routledge Handbook of Science, Technology, and Society*, (January 2014), pp. 173–188.

Reynolds, L. & Scott, R., 2016. Digital Citizens: Countering Extremism Online, *Institute for Strategic Dialogue*.

Reynolds, S.C. & Hafez, M.M., 2017. Social Network Analysis of German Foreign Fighters in Syria and Iraq. *Terrorism and Political Violence*, 31(4), pp. 661-686.

Ribeiro, M.H. et al., 2019. Auditing Radicalization Pathways on YouTube. *Woodstock '18: ACM Symposium on Neural Gaze Detection*.

Richards, A., 2015. From Terrorism to "Radicalization" to "Extremism": Counterterrorism imperative or loss of focus? *International Affairs*, 91(2), pp.371–380.

Rieger, D., Frischlich, L. & Bente, G., 2013. *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*, Köln: Wolters Kluwer.

Rieger, D., Frischlich, L. & Bente, G., 2017. Propaganda in an Insecure, Unstructured World: How psychological uncertainty and authoritarian attitudes shape the evaluation of right-wing extremist internet propaganda. *Journal for Deradicalization*, 10, pp.203–229.

Robinson, M.D. & Dauber, C.E., 2018. Grading the Quality of ISIS Videos: A Metric for Assessing the Technical Sophistication of Digital Video Propaganda. *Studies in Conflict and Terrorism*, 42(1–2), pp.70–87.

Rosenblatt, N., Winter, C. & Basra, R., 2019. Islamic State Propaganda and Attacks: How Are They Connected? *Perspectives on Terrorism*, 13(5), pp.39–60.

Rowe, I., 2015. Civility 2.0 : A Comparative Analysis of Incivility in Online Political Discussion. *Information, Communication & Society*, 18(2), pp.121–138.

Rutte, M., 2017, Short Speech by Prime Minister Mark Rutte for the Side Event on Online Radicalisation, *Government of the Netherlands*, Available at: https://www.government.nl/government/members-of-cabinet/mark-rutte/documents/speeches/2017/09/20/short-speech-by-prime-minister-mark-rutte-for-the-side-event-on-online-radicalisation.

Safer-Lichtenstein, A., LaFree, G. & Loughran, T., 2017. Studying Terrorism Empirically: What We Know About What We Don't Know. *Journal of Contemporary Criminal Justice*, 33(3), pp.273–291.

Sageman, M., 2008a. *Leaderless Jihad: Terror Networks in the Twenty-first Century*, Philadelphia: PA: University of Pennsylvania Press.

Sageman, M., 2008b. The Next Generation of Terror. *Foreign Policy*, (March/April), pp.36–42.

Sageman, M., 2004. *Understanding Terror Networks*, Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. (2014) 'The Stagnation in Terrorism Research', *Terrorism and Political Violence*, 26(4), pp. 565–580.

Saifudeen, O. A., 2014. The Cyber Extremism Orbital Pathways Model, *RSIS Working Paper.*

Saltman, E.M. & Smith, M., 2015. "Till Martyrdom Do Us Part": Gender and the ISIS Phenomenon. *Institute for Strategic Dialogue*.

Schmid, A.P., 2015. Challenging the Narrative of the "Islamic State." *International Centre for Counter-Terrorism*.

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

Schmid, A.P., 2004. Terrorism - The Definitional Problem. *Case Western Reserve Journal of International Law*, 36(2), pp.375–419.

Scrivens, R., Gill, P., and Conway, M., 2020. The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research, in: Holt, T.J. and Bossler, A. [Eds.], *Palgrave Handbook of International Cybercrime & Cyberdeviance*, London: Palgrave.

Schmitt, G.R. & Konfrst, H.J., 2015. Life Sentences in the Federal System. *United States Sentencing Commission*.

Schuurman, B. et al., 2017. End of the Lone Wolf: The Typology that Should Not Have Been. *Studies in Conflict & Terrorism*. 42(8), pp.771-778.

Schuurman, B. et al., 2018. Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis,. *Journal of Forensic Sciences*, 63(4), pp. 1191-1200.

Schuurman, B. & Taylor, M., 2018. Reconsidering Radicalization: Fanaticism and the Link Between Ideas and Violence. *Perspectives on Terrorism*, 12(1), pp.3–22.

Schuurman, B., 2018. Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship, *Terrorism and Political Violence.*

Sedgwick, M., 2010. The Concept of Radicalization as a Source of Confusion. *Terrorism and Political Violence*, 22(4), pp.479–494.

Shane, S., 2016a. Anwar al-Awlaki's Life After Death. *Foreign Policy*, May 10. Available at: http://foreignpolicy.com/2016/05/10/anwar-al-awlaki-yemen-obama/.

Shane, S., 2016b. The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State. *CTC Sentinel*, 9(7), pp.15–20.

Shehabat, A. & Mitew, T., 2018. Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 12(1), pp.81–99.

Silber, M.D. & Bhatt, A., 2007. Radicalization in the West: The homegrown threat. *New York City Police Department*.

Silva, D.M.D., 2018. "Radicalisation: the Journey of a Concept", Vevisited. *Race and Class*, 59(4), pp.34–53.

Sivek, S.C., 2013. Packaging Inspiration: Al Qaeda's digital magazine inspire in the self-radicalization process. *International Journal of Communication*, 7(1), pp.584–606.

Skinner, C., 2015. Punishing Crimes of Terror in Article III Courts. *Yale Law & Policy Review*, 31(2).

Slater, D. 2002. Social relationships and identity online and offline. In: Lievrouw, L., and Livingstone, S. *Handbook of new media: Social shaping and consequences of ICTs*. London: Sage; 553-546.

Snow, D. & Cross, R., 2011. Radicalism within the Context of Social Movements: Processes and Types. *Journal of Strategic Security*, 4(4), pp.115–130.

Soufan Group, 2015. Foreign Fighters - An Updated Assessment of the Flow of Foreign Fighters to Syria and Iraq.

Spears, R., et al., 2002. Computer-mediated communication as a channel for social resistance: The strategic side of SIDE. *Small Group Research*, 33; 555-574.

START, 2018. Profiles of Individual Radicalization in the United States (PIRUS) Codebook. Available at: www.start.umd.edu.

START, nd. Global Terrorism Database. Available at: https://www.start.umd.edu/gtd/.

Statistica, 2019, Number of Social Media Users Worldwide 2010-2021, Available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

Stern, J. & Berger, J.M., 2015. *ISIS: The State of Terror*, New York, NY: HarperCollins.

Stohl, M., 2008. Old Myths, New fantasies and the Enduring Realities of Terrorism. *Critical Studies on Terrorism*, 1(1), pp.5–16.

Strauss, A. and Corbin, J., 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage Publications: Newbury Park, CA, USA.

Stroud, N.J., Peacock, C. & Curry, A.L., 2019. The Effects of Mobile Push Notifications on News Consumption and Learning. *Digital Journalism*.

Suler, J., 2004. The Online Disinhibition Effect. *CyberPsychology & Behavior*, 7(3), pp.321–326.

Sunstein, C. R., 2001. *Republic.com*. Princeton, NJ: Princeton University Press.

Sunstein, C. R., 2002. The law of group polarization, *The Journal of Political Philosophy*, 10(2), pp. 175–195.

Sutherland, E. H., 1947. *Principles of Criminology*, 4th edn. Chicago: Lippincott.

Tech Against Terrorism, nd. Home. Available at: https://www.techagainstterrorism.org/.

Tech Against Terrorism, 2019. ISIS use of smaller platforms and the DWeb to share terrorist content Summary. April 29. Available at: https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/.

Terrorism Content Analytics Platform, nd. Group Inclusion Policy. Available at: https://www.terrorismanalytics.org/group-inclusion-policy.

The Camstoll Group, 2016. Use of Social Media By Terrorist Fundraisers and Financiers.

The Fund for Peace, 2019. Fragile States Index Annual Report 2019.

Thornton, A. & Bouhana, N., 2017. Preventing Radicalization in the UK: Expanding the Knowledge-Base on the Channel Programme. *Policing: A Journal of Policy and Practice*, pp.1–14.

Thorseth, M. 2015a. Commentary of the Manifesto, in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 37-40.

Thorseth, M. 2015b. On Tolerance and Fictitious Publics, in: Floridi, L. [Ed.] *The Onlife Manifesto: Being Human in a Hyperconnected Era*, London: SpringerOpen, pp. 245-260.

Torres-Soriano, M.R., 2016. The Hidden Face of Jihadist Internet Forum Management: The Case of Ansar Al Mujahideen. *Terrorism and Political Violence*, 28(4), pp.735–749.

Torok, R., 2013. Developing an explanatory model for the process of online radicalisation and terrorism, *Security Informatics*, 2(6), pp. 1–10.

Tuck, H. & Silverman, T., 2016. The Counter-narrative Handbook. *Institute for Strategic Dialogue*.

Tufekci, Z., 2018, YouTube, the Great Radicalizer, *New York Times,* March 10, Available at: https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

Turner, J., 2015. Strategic differences: Al Qaeda's Split with the Islamic State of Iraq and al-Sham. *Small Wars and Insurgencies*, 26(2), pp.208–225.

Uimonen, P., 2013. Visual Identity in Facebook. *Visual Studies*, 28(2), pp.122–135.

United Nations Counter Terrorism Executive Directorate, 2015. Analysis and recommendations with regard to the global threat from foreign fighters.

United Nations Security Council, 2014, Resolution 2178, Available at:

https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29.

United Nations Security Council, 2015, Resolution 2253, Available at: https://www.un.org/securitycouncil/content/un-sc-consolidated-list.

Urquhart, C., Lehmann, H. and Myers, M.D., 2010. Putting the 'Theory' Back into Grounded Theory: Guidelines for grounded theory studies in information systems, *Information Systems Journal,* 20(4), pp. 357-381.

Urquhart, C., 2013. *Grounded Theory for Qualitative Research: A Practical Guide*, London: Sage Publications.

Valentini, D., Lorusso, A. M. and Stephan, A., 2020. Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization, *Frontiers in Psychology.*

Varvelli, A., 2016. *Jihadist Hotbeds: Understanding Local Radicalization Processes* A. Varvelli, [ed.], Milan: Italian Institute for International Political Studies.

Vatcheva, K. P., & Lee, M., 2016. Multicollinearity in Regression Analyses Conducted in Epidemiologic Studies, *Epidemiology*, 6(2), pp.1-20.

Veldhuis, T. & Staun, J., 2009. *Islamist Radicalisation: A root cause model*. Clingendael Institute.

Venhaus, J.M., 2010. Why Youth Join al-Qaeda. *United States Institute Of Peace*, Special Report, pp.1–20.

Del Vicario, M., Vivaldo, G., *et al.* (2016) 'Echo Chambers: Emotional Contagion and Group Polarization on Facebook', *Nature Publishing Group*, pp. 1–14.

Del Vicario, M., Bessi, A., *et al.* (2016) 'The spreading of misinformation online', *Proceedings of the National Academy of Sciences*, 113(3), pp. 554–559.

Victoroff, J., 2005. The Mind of the Terrorist: A Review and Critique of Psychological Approaches. *Journal of Conflict Resolution*, 49(1), pp.3–42.

Vidino, L. & Hughes, S., 2015. ISIS in America: From Retweets to Raqqa, *George Washington University Program on Extremism*.

Vidino, L. Harrison, S., & Spada, C. 2016. ISIS and al-Shabaab in Minnesota's Twin Cities: the American Hotbed, in: Varvelli, A. [Ed.], *Jihadist Hotbeds: Understanding Local Radicalization Processes*, Milan: Italian Institute for International Political Studies.

Vidino, L., Marone, F. & Entenmann, E., 2017. *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West*, Milan: Ledizioni.

Van Vlierden, G. 2016. The Brussels-Antwerp Axis as Hotbed of Belgian Jihad, in: Varvelli, A. [Ed.], *Jihadist Hotbeds: Understanding Local Radicalization Processes*, Milan: Italian Institute for International Political Studies.

Vyas, P., 2017. The Islamic State's Married Ideology: Something Borrowed, Something New. *Lawfare Blog*, (July 2). Available at: https://www.lawfareblog.com/islamic-states-married-ideology-something-borrowed-something-new.

Walther, J. B. 1996. Computer-Mediated Communication Impersonal, Interpersonal, and Hyper- personal Interaction. *Communication Research*, 23(1): 3-43

Waters, G. & Postings, R., 2018. Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook, *Counter Extremism Project.*

Watkin, A.-L. & Looney, S., 2018. "The Lions of Tomorrow": A News Value Analysis of Child Images in Jihadi Magazines. *Studies in Conflict & Terrorism*, 42(1-2), pp. 120-140.

Webb, E., 2017. *Spotting the Signs : Identifying Vulnerability to Radicalisation Among Students*, Henry Jackson Society.

Webber, D. et al., 2018. The Road to Extremism: Field and experimental evidence that significance loss-induced need for closure fosters radicalization. *Journal of Personality and Social Psychology*, 114(2), pp.270–285.

Webber, D. & Kruglanski, A., 2017. Psychological Factors in Radicalization: A "3 N" Approach. In G. LaFree & J. D. Freilich, eds. *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 33–46.

Webber, D. & Kruglanski, A., 2018. The Social Psychological Makings of a Terrorist. *Current Opinion in Psychology*, 19, pp.131–134.

Weimann, G. and Von Knop, K., 2008. 'Applying the Notion of Noise to Countering Online Terrorism', *Studies in Conflict & Terrorism*, 31, pp. 883–902

Weimann, G., 2012. Lone Wolves in Cyberspace. *Journal of Terrorism Research*, 3(2), pp.75–90.

Weirman, S. & Alexander, A., 2018. Hyperlinked Sympathizers: URLs and the Islamic State. *Studies in Conflict & Terrorism*.

West, L.J., 2016. # jihad : Understanding Social Media as a Weapon. *Security Challenges*, 12(2), pp.9–26.

Whiteside, C., 2016. New Masters of Revolutionary Warfare: The Islamic State Movement (2002-2016). *Perspectives on Terrorism*, 10(4), pp.6–20.

Whittaker, J., 2018. Online Radicalization, the West, and the "Web 2.0": A Case Study Analysis, in: Minchev, Z. and Bogdanoski, M. [Eds.], *Countering Terrorist Activities in Cyberspace*, Amsterdam: IOS Press, pp. 106-120.

Whittaker, J., 2020. 'Online Echo Chambers and Violent Extremism', in Khasru, S. M. and Noor, R. (eds) *The Digital Age, Cyber Space, and Social Media: The Challenges of Security & Radicalization*. Dhaka: Institute for Policy, Advocacy, and Governance, pp. 129–150

Wignell, P., Tan, S., O 'Halloran, K.L., et al., 2017. A Mixed Methods Empirical Examination of Changes in Emphasis and Style in the Extremist Magazines Dabiq and Rumiyah. *Perspectives on Terrorism*, 11(2), pp.2–20.

Wignell, P., Tan, S. & O'Halloran, K.L., 2017. Under the Shade of AK47s: A multimodal

approach to violent extremist recruitment strategies for foreign fighters. *Critical Studies on Terrorism*, 10(3), pp.1–24..

Wikström, P.O.H. & Bouhana, N., 2017. Analyzing Radicalization and Terrorism: A Situational Action Theory. In G. LaFree & J. D. Freilich, eds. *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 175–186.

Wiktorowicz, Q., 2006. Anatomy of the Salafi movement. *Studies in Conflict and Terrorism*, 29(3), pp.207–239.

Wiktorowicz, Q., 2013, Working to Counter Online Radicalization to Violence in the United States, *White House Blog*, Available at: https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counter-online-radicalization-violence-united-states

Wilbur, D., 2017. Propaganda's Place in Strategic Communication: The Case of ISIL's Dabiq Magazine. *International Journal of Strategic Communication*, pp.1–15.

Williams, B. 2011. On the Trail of the 'Lions of Islam': Foreign Fighters in Afghanistan and Pakistan, 1980-2010, *Foreign Policy Research Institute,* pp. 216-239.

Windisch, S. et al., 2018. Understanding the Micro-Situational Dynamics of White Supremacist Violence in the United States. *Perspectives on Terrorism*, 12(6), pp.23–37.

Winkler, C. et al., 2018. Images of death and dying in ISIS media: A comparison of English and Arabic print publications. *Media, War & Conflict*, pp.1–15.

Winter, C., 2015a. Detailed Analysis of Islamic State Propaganda Video: Although the Disbelievers Dislike It. *Quilliam Foundation*.

Winter, C., 2015b. Documenting the Virtual "Caliphate." *Quilliam Foundation*.

Winter, C., 2017. Media Jihad: The Islamic State's Doctrine for Information Warfare. *International Centre for the Study of Radicalisation and Political Violence*.

Winter, C., 2015c. The Virtual "Caliphate": Understanding Islamic State's Propaganda Strategy, *Quilliam Foundation*.

Winter, C., 2018. Totalitarian Insurgency: Evaluating the Islamic State's In-Theatre Propaganda Options, *US Naval War College*, Newport, Rhode Island.

Wojcieszak, M., 2008. False Consensus goes Online Impact of Ideologically Homogeneous Groups on False Consensus. *Public Opinion Quarterly*, 72(4), pp.781–791.

Woodring, D., 2014. *21st Century Radicalization: The Role of the Internet User and Nonuser in Terrorist Outcomes*. University of Arkansas, Fayetteville.

Zelin, A.Y., 2015. Picture Or It Didn't Happen : A Snapshot of the Islamic State's Official Media Output. *Perspectives on Terrorism*, 9(4), pp.85–97.

Statutes Cited

18 U.S.C. §2331, 2001

18 U.S.C §2338A, 2009

18 U.S.C §2339B, 2015

European Parliament, General Data Protection Regulation, 2018, Available at: https://gdpr-info.eu/.

HM Parliament, Counter-Terrorism and Border Security Act 2019, c.3. Available at: http://www.legislation.gov.uk/ukpga/2019/3/contents/enacted.

Cases Cited

USA v. Zakaryia Abdin, Criminal Complaint, Case: 2:17-mj-00081-MCRI, United States District Court for the District of South Carolina, 2017.

USA v. Mahad Abdiaziz Abdiraham. Criminal Complaint, 4th Judicial District Court, Case: 27-CR-17-28647. State of Minnesota, County of Hennepin, 2017.

USA v. Abdullahi Ahmed Abdullahi, Indictment, Case 3:17-cr-00622-W, United States District Court for the Southern District of California, 2017.

USA v. Munir Abdulkader, Sentencing Proceedings, Case 1:16-CR-019, United States District Court for the Southern District of Ohio, Western Division, 2016.

USA v. Hamza Naj Ahmed et al, Superseding Indictment, Case 0:15-cr-00049, United States District Court for the District of Minnesota, 2015.

USA v. Laith Waleed Alebbini, Motion to Revoke Detention Order, United States District Court for the Southern District of Ohio, Case: 317-cr-00071-WHR, 2017.

USA v. Mohommad Hasnain Ali, Factual Basis, Case 4:17-cr-00087-MAC-CA, United States District Court for the Eastern District of Texas, Sherman Division, 2017.

USA v. Sajmir Alimehmeti, Criminal Complaint, Case: 1:16-cr-00398, United States District Court for the Southern District of New York, 2016.

USA v. Ali Shukri Amin, Defendant's Sentencing Memorandum, Case: 1:15-cr-00164-CMH, United States District Court for the Eastern District of Virginia, Alexandria Division, 2015.

USA v. Ali Shukri Amin, Position Of The United States With Respect To Sentencing, Case 1:15-cr-00164-CMH, United States District Court for the Eastern District of Virginia, 2015.

USA v. Ali Shukri Amin, Statement of Facts, Case: 1:15-cr-00164-CMH, United States District Court for the Eastern District of Virginia, Alexandria Division, 2015.

USA v. Jalil ibn Ameer Aziz, Government's Sentencing Memorandum, Case 1:15-cr-00309-CCC, United States District Court for the Middle District of Pennsylvania, 2017.

USA v. Matin Azizi-Yarand, Affidavit for Arrest Warrant, Case Number: 18045858, United States District Court for the Eastern District of Texas, 2018.

USA v. Abdulrahman El Bahnasawy, Criminal Complaint, Case: 1:16-cr-00376, United States District Court for the Southern District of New York, 2016.

USA v. Abdurahman El Bahnasawy, Handwritten Letter, Case 1:16-cr-00376-RMB, United States District Court for the Southern District of New York, 2016.

USA v. Mohimanul Bhuiya, Criminal Complaint, Case 1:14-cr-00612-JBW-RLM, United States District Court for the Eastern District of New York, 2014.

USA v. John T. Booker Jr. Criminal Complaint, Case 5:15-mj-05039-KGS, United States District Court for the District of Kansas, Topeka Docket, 2015.

USA v. Clark Calloway, Criminal Complaint, Case 1:17-mj-00287-GMH, United States District Court for the District of Columbia, 2017.

USA v. Marie Antoinette Castelli, Plea Agreement, Case: 2:17-cr-00049-DLB, United States District Court for the Eastern District of Kentucky, 2017.

USA v. Heather Coffman, Defendant's Position on Sentencing, Case 3:15-cr-00016-JAG, United States District Court for the Eastern District of Virginia, 2015.

USA v. Heather Coffman, Position of the US on Sentencing, Case: 3:15-cr-00016, United States Court for the Eastern District of Virginia, 2015.

USA v. Heather Coffman, Statement of Facts, Case 3:15-cr-00016-JAG, United States District Court for the Eastern District of Virginia, 2015.

USA v. Shannon Maureen Conley, Criminal Complaint, Case: 1:14-mj-01045-KLM, United States District Court for the District of Colorado, 2014.

USA v. Shannon Maureen Conley, Information, Case: 1:14-mj-01045-KLM, United States District Court for the District of Colorado, 2014.

USA v. Christopher Lee Cornell, Government's Sentencing Memorandum, Case: 1:15-cr-00012-SSB, United States District Court for the Southern District of Ohio, Western Division, 2016.

USA v. Waheba Issa Dais, Affidavit in Support of Criminal Complaint, Case 2:18-cr-00143, United States District Court for the Eastern District of Wisconsin, 2018.

USA v. Muhammad Oda Dakhlalla, Factual Basis, Case: 1:15-cr-00098-SA-DAS, United States District Court for the Northern District of Mississippi, 2016.

USA v. Nelash Mohamed Das, Criminal Complaint, Case: 8:16-cr-00502, United States District Court for the District of Maryland, 2016.

USA v. John Doe, Sentencing, Case 1:15-cr-00302-MKB, United States District Court for the Eastern District of New York, 2016.

USA v. Sean Andrew Duncan, Application for a Search Warrant, Case 1:18-sw-00029-IDD, United States District Court for the Eastern District of Virginia, 2017.

USA v. Mufid A. Elfgeeh, Affidavit, Case: 6:15-cr-06052, Unites States District Court for the Western District of New York, 2016.

USA v. Mahmoud Amin Mohamed Elhassan, Government Sentencing Memorandum, Case 1:16-cr-00064-AJT, United States District Court for the Eastern District of Virginia, 2017.

USA v. Nader Salem Elhuzayel and Muhanad Elfatih M.A. Badawi, Transcript of Proceedings, Case 8:15-cr-0060, United States District Court for the Central District of California, 2016.

USA v. Mohamed Elshinawy, Criminal Complaint, Case 1:16-cr-00009-ELH, United States District Court for the District of Maryland, 2015.

USA v. Mohamed Elshinawy, Plea Agreement, Case 1:16-cr-00009-ELH, United States District Court for the District of Maryland, 2017.

USA v. Mohamed Abdihamid Farah et al, Criminal Complaint, Case 0:15-cr-00049, United States District Court for the District of Minnesota, 2015.

USA v. Ahmed Mohammed el Gammal, Criminal Complaint, Case 1:15-cr-00588-ER, United States District Court for the Southern District of New York, 2015.

USA v. Joshua Ray van Haften, Government Sentencing Memorandum, Case: 3:15-cr-00037-jdp, United States District Court for the Western District of Wisconsin, 2017.

USA v. Robert Lorenzo Hester Jr., Criminal Complaint, Case: 4:17-cr-00064, United States District Court for the Western District of Missouri, 2017.

USA v. Ramiz Hodzic et al. Government's Response in Opposition to Defendant's Motion to Dismiss, Case: 4:15-cr-00049-CDP-DDN, United States District Court for the Eastern District of Missouri, Eastern Division, 2015.

USA v. Gregory Hubbard, Dayne Antani Christian, and Darren Arness Jackson, Criminal Complaint, Case 9:16-cr-80107, United Staes District Court for the Southern District of Florida, 2016.

USA v. Yusra Ismail, Criminal Complaint, Case 0:14-mj-01047-JSM, United States District Court for the District of Minnesota, 2014.

USA v. Mohamed Bailor Jalloh, Criminal Complaint, Case 1:16-mj-00296-TCB, United States District Court for the Eastern District of Virginia, 2016.

USA v. Everitt Aaron Jameson, Criminal Complaint, Case 1:18-cr-00001, United States District Court for the Eastern District of California, 2017.

USA v. Aws Mohammed Younis al-Jayab, Criminal Complaint, Case 1:18-cr-00721, United States District Court for the Northern District of Illinois, 2016.

USA v. Joseph Jones and Edward Schimenti, Criminal Complaint, Case 1:17-cr-00236, United States District Court for the Northern District of Illinois, 2017.

USA v. Abdurasul Juraboev et al., Criminal Complaint, United States District Court for the Eastern District of New York, Case: 1:15-cr-00095, 2015.

USA v. Abdurasul Hasanovich Juraboev et al., Defendant's Sentencing Memorandum, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York

USA v. Abdurasul Juraboev et al., Superseding Indictment, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York, 2015.

USA v. Abdul Malik Abdul Kareem, Exhibit List, Case 2:15-cr-00707-SRB, United States Court for the District of Arizona, 2016.

USA v. Abdul Malik Abdul Kareem, Second Superseding Indictment, Case 2:15-cr-00707-SRB, United States District Court for the District of Arizona, 2015.

USA v. Abdul Malik Abdul Kareem, Government's Sentencing Memorandum, Case 2:15-cr-00707-SRB, United States District Court for the District of Arizona, 2016.

USA v. Asher Abid Khan, Criminal Complaint, Case: 4:15-cr-00263, United States District Court for the Southern District of Texas, 2015.

USA v. Dilshod Khusanov, Detention Request, Case: 1:17-cr-00475-WFK-SMG, United States District Court for the Eastern District of New York, 2017.

USA v. Mohamed Jamal Khweis, Criminal Complaint, Case 1:16-mj-00213-JFA, United States District Court for the Eastern District of Virginia, 2016.

USA v. Mohamed Jamal Khweis, Government's Amended Trial Exhibit List (June 1, 2017), Case 1:16-cr-00143-LO, United States District Court for the Eastern District of Virginia, 2017.

USA v. Mohamed Jamal Khweis, Government's Sentencing Memorandum, Case 1:16-cr-00143-LO, United States District Court for the Eastern District of Virginia, 2017.

USA v. Gregory Lepsky, Criminal Complaint, Case 3:18-cr-00114, United States District Court, District of New Jersey, 2017.

USA v. Jason Ludke and Yosvany Padilla-Conde, Criminal Complaint, Case: 1:16-mj-00053, United States District Court for the Eastern District of Wisconsin, 2016.

USA v. Enrique Marquez Jr., Criminal Complaint, Case: 5:15-mj-498, United States District Court for the Central District of California, 2015.

USA v. Terrence Joseph McNeil, Affidavit, Case: 5:15-mj-01176-KBB, United States District Court for the Northern District of Ohio, 2015.

USA v. Donald Ray Morgan, Factual Basis, Case 1:14-cr-414-1, United States District Court for the Middle District of North Carolina, 2014.

USA v. Fareed Mumuni, Criminal Complaint, Case 1:15-mj-00554-VMS, United States District Court for the Eastern District of New York, 2015.

USA v. Arafat M. Nagi, Criminal Complaint, Case 1:15-cr-00148, United States District Court for the Western District of New York, 2015.

USA v. Mohamed Rafik Naji, Criminal Complaint, Case 1:16-cr-00653, United States District Court for the Eastern District of New York, 2016.

USA v. Islam Said Natsheh, Defendant's Sentencing Memorandum, Case 3:16-cr-00166, United States District Court for the Northern District of California, 2016.

USA v. Islam Said Natsheh, Government's Sentencing Memorandum, Case: 3:16-cr-00166-RS, United States District Court for the Northern District of California, 2016.

USA v. Shivam Patel, Government's Sentencing Memorandum, Case 2:17-cr-00120-MSD-DEM, United States District Court for the Eastern District of Virginia, 2018.

USA v. Shivam Patel, Affidavit in Support of an Application for Criminal Complaint and Arrest Warrant, Case 2:17-cr-00120-MSD-DEM, United States District Court for the Eastern District of Virginia, 2017.

USA v. Haris Qamar, Government's Sentencing Memorandum, Case 1:16-cr-00227-LMB, United States District Court for the Eastern District of Virginia, 2017.

USA v. Haris Qamar, Statement of Facts, Case 1:16-cr-00227-LMB, United States District Court for the Eastern District of Virginia, 2016.

USA v. Saddam Mohamed Raishani, Criminal Complaint, Case: 1:17-cr-00421, United States District Court for the Southern District of New York, 2017.

USA v. Ahmed Khan Rahimi, Criminal Complaint, Case 1:16-cr-00760-RMB, 2016.

USA v. Ahmed Khan Rahimi, Government's Sentencing Memorandum, Case 1:16-cr-00760-RMB, United States District Court, District of New Jersey, 2018.

USA v. Mohamed Amiin Ali Roble, Criminal Complaint, Case 0:16-mj-00584, United States District Court for the District of Minnesota, 2016.

USA v. Nicholas Rovinski, Government's Sentencing Memorandum, Case 1:15-cr-10153-WGY, United States District Court for the District of Massachusetts, 2017.

USA v. Alaa Saadeh, Criminal Complaint, [Unknown case #], United States District Court for the District of New Jersey, 2015. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Saadeh%2C%20A.%20Criminal%20Complaint.pdf.

USA v. Nader Saadeh, Criminal Complaint, Case 2:15-cr-00618, United States District Court for the District of New Jersey, 2015.

USA v. Ashraf al Safoo, Criminal Complaint, Case 1:18-cr-00696, United States District Court for the Northern District of Illinois, Eastern Division, 2018.

USA v. Akhror Saidahkmetov, Defendant's Sentencing Memorandum, Case 1:15-cr-00095-WFK, United States District Court for the Eastern District of New York, 2017.

USA v. Akhror Saidakhmetov, Government's Sentencing Memorandum, United States District Court for the Eastern District of New York, Case 1:15-cr-00095-WFK, 2017.

USA v. Sayfullo Saipov, Criminal Complaint, Case 1:17-mj-08177, United States District Court for the Southern District of New York, 2017.

USA v. Munther Saleh, Defendant's Sentencing Memorandum, Case 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018.

USA v. Munther Omar Saleh, Government's Response to Defendant's Sentencing Memorandum, Case 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018.

USA v. Munther Omar Saleh and Fareed Mumuni, Government's Sentencing Memorandum, Case 1:15-cr-00393-MKB, United States District Court for the Eastern District of New York, 2018.

USA v. Khalil Abu Rayyan, Criminal Complaint, Case: 2:16-mj-30039-DUTY, United States District Court for the Eastern District of Michigan, 2016

USA v. Russel Salic, Criminal Complaint, [No Case Number], United States District Court for the Southern District of New York, 2016.

USA v. Mediha Medy Salkicevic, Detention Hearing, Case: 4:15-cr-00049-CDP-DDN, United States District Court for the Eastern District of Missouri, 2015.

USA v. Noor Salman, Defendant's Motion to Preclude Improper Argument in Government's Opening Statement, Case 6:17-cr-00018-PGB-KRS, United States District Court for the Middle District of Florida, Orlando Division, 2018.

USA v. Noor Salman, Government's Motion for an Order Revoking Defendant's Release, Case 6:17-cr-00018-PGB-KRS, United States District Court for the Middle District of Florida, Orlando Division, 2017.

USA v. Aziz Ihab Sayyed, Criminal Complaint, Case 5:18-cr-00090-AKK-HNK, United States District Court for the Northern District of Alabama, 2018.

USA v. Aziz Ihab Sayyed, Plea Agreement, Case 5:18-cr-00090-AKK-HNJ, United States District Court for the Northern District of Alabama, 2018.

USA v. Zoobia Shahnaz, Indictment, Case: 2:17-cr-00690, United States District Court for the Eastern District of New York, 2017.

USA v. Casey Charles Spain, Position of The United States with Respect to Sentencing and Motion for an Upward Variant Sentence, Case 3:17-cr-00123-JAG, United States District Court for the Eastern District of Virginia, 2017.

USA v. Casey Charles Spain, Defendant's Sentencing Position, Case 3:17-cr-00123-JAG, United States District Court for the Eastern District of Virginia, 2018.

USA v. Harlem Suarez, Criminal Complaint, Case 0:15-mj-05016-LSS, United States District Court for the Southern District of Florida, 2015.

USA v. Harlem Suarez, Government's Sentencing Memorandum, Case 4:15-cr-10009-JEM, United States District Court for the Southern District of Florida, 2017.

USA v. Justin Nojan Sullivan, Factual Basis, Case No. 1:16-cr-05- MR-DLH, United States District Court for the Western District of North Carolina, 2016.

USA v. Nicholas Teausant, Criminal Complaint, Case 2:14-mj-0064, United States District Court for the Eastern District of California, 2014.

USA v. Keonna Thomas, Criminal Complaint, Case: 2:15-cr-00171, United States District Court for the Eastern District of Pennsylvania, 2015.

USA v. Keonna Thomas, Defendant's Sentencing Memorandum, Case 2:15-cr-00171-MMB, United States Court for the Eastern District of Pennsylvania, 2017.

USA v. Keonna Thomas, Government's Sentencing Memorandum, Case 2:15-cr-00171-MMB, United States Court for the Eastern District of Pennsylvania, 2017.

State of Arizona v. Derrick Raymond Thompson, Direct Complaint, Superior Court for the State of Arizona, County of Maricopa, Case No: CR2016-159174-001, 2016.

USA v. Samuel Topaz, Criminal Complaint, Case 2:15-cr-00450, United States District Court for the District of New Jersey, 2015.

USA v. Akayed Ullah, Criminal Complaint, Case: 1:17-mj-09200-UA, United States District Court for the Southern District of New York, 2017.

USA v. Noelle Velentzas and Asia Siddiqui, Criminal Complaint, Case 1:15-mj-00303-VVP, United States District Court for the Eastern District of New York, 2015.

USA v. Abdirizak Warsame, Criminal Complaint, Case 0:15-mj-00978-HB, United States District Court for the District of Minnesota, 2015.

USA v. Lionel Nelson Williams, Statement of Facts, Case 2:17-cr-00001-AWA-LRL, United States District Court for the Eastern District of Virginia, 2017.

USA v. David Wright and Nicholas Rovinski, Affidavit, Case 1:15-cr-10153-WGY, United States District Court District of Massachusetts, 2015.

USA v. David Wright and Nicholas Rovinski, First Superseding Indictment, Case 1:15-cr-10153-WGY, United States District Court for the District of Massachusetts, 2016.

USA v. Safya Rose Yassin, Criminal Complaint, Case: 16-3024-01-CR-S-RK, United States District Court for the Western District of Missouri, 2016.

USA v. Safya Roe Yassin, Superseding Indictment, Case No. 16-3024-01-CR-S-MDH, United States District Court for the Western District of Missouri, 2016.

USA v. Safya Roe Yassin, Transcript of Hearing on Initial Appearance, Case No. 16-03024-01-CR-S-MDH, United States District Court for the Western District of Missouri Southern Division, 2016.

USA v. Jaelyn Delshaun Young and Muhammad Oda Dakhlalla, Criminal Complaint, Case: 3:15-mj-32-SAA, 2015.

USA v. Nicholas Young, Application for Search Warrant, Case 1:17-sw-00733-TCB, United States District Court for the Eastern District of Virginia, 2017.

USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint, Case: 14-MJ-0124, United States District Court for the District of Minnesota, 2014.

USA v. Abdullahi Yusuf, Change of Plea Hearing, Case 0:15-cr-00046-MJD, United States District Court for the District of Minnesota, 2015.

Media Sources Cited

Aaronson, T., How the FBI Created a Terrorist, *The Intercept*, March 16, 2015. Available at: https://theintercept.com/2015/03/16/howthefbicreatedaterrorist/.

Abutaleb, Y. and Cooke, K., A teen's turn to radicalism and the US safety net that failed to stop it, *Reuters*, June 6, 2016. Available at: https://www.reuters.com/investigates/special-report/usa-extremists-teen/.

Alexander, H. New York Woman Charged with Sending $85,000 in Bitcoin to Support ISIL, *The Telegraph*, December 14 2017. Available at: https://www.telegraph.co.uk/news/2017/12/14/new-york-woman-charged-sending-85000-bitcoin-support-isil/.

Al-Jezairy, A., How Online Radicalization Is Drawing Young Western Women to the Islamic State, *Vice News*, Febuary 2, 2015., Available at: https://www.vice.com/en_us/article/j547gg/how-online-radicalization-is-drawing-young-western-women-to-the-islamic-state.

Amin, A.S., Bitcoin wa' Sadaqat al-Jihad, 2014 Available at: https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf.

Ashton, A., Suspected ISIS Sympathiser from Montesano was Hospitalized for Mental Health Problems, Records Show, *The News Tribune,* 12 Feb 2016. Available at: https://www.thenewstribune.com/news/local/military/article60143536.html.

Aslanian, S., Yuen, L. and Ibrahim, M., Called to Fight: Minnesota's ISIS Recruits, *MPR News*, 25 March 2015. Available at: https://www.mprnews.org/story/2015/03/25/minnesota-isis#yismail.

Associated Press, 'I am an American': Man who was 'ready for jihad' before attempting to join ISIL sobs as he's given 15 years in prison, *National Post*, July 28, 2015. Available at: http://nationalpost.com/news/world/i-am-an-american-man-who-was-ready-for-jihad-before-attempting-to-join-isil-sobs-as-hes-given-15-years-prison.

Associated Press, Man Accused of Shooting Philly Officer Convicted of Attempted Murder, *ABC News*, Febuary 1, 2018, http://6abc.com/man-accused-of-shooting-philly-officer-found-guilty/3018942/.

Baker, A., and Santora, S., San Bernardino Attackers Discussed Jihad in Private Messages, FBI Says, *New York Times*, December 16, 2015. Available at: https://www.nytimes.com/2015/12/17/us/san-bernardino-attackers-discussed-jihad-in-private-messages-fbi-says.html.

BBC News, Paris Attacks: What Happened on the Night, December 9, 2015, Available at: https://www.bbc.co.uk/news/world-europe-34818994.

BBC News, San Bernardino Shooting: The Story of the Attack, December 5, 2015, Available at: https://www.bbc.co.uk/news/av/world-us-canada-34991990/san-bernardino-shooting-the-story-of-the-attack

BBC News, Tunisia Attack on Sousse Beach 'Kills 39', June 27, 2015, Available at: https://www.bbc.co.uk/news/world-africa-33287978.

BBC News, US Unemployment Rate Falls to 50-year Low of 3.5%, October 4, 2019. Available at: https://www.bbc.co.uk/news/business-49934309.

CBC News, Canadian Convicted of Terrorism in US asks for 2nd Chance, March 3, 2018. Available at: http://www.cbc.ca/news/world/canadian-convicted-of-terrorism-in-u-s-asks-for-2nd-chance-1.4561306.

CBS Philadelphia, Edward Archer Sentenced Up to 97 Years in Prison for Shooting Officer Jesse Hartnett in the Name of ISIS, May 14, 2018. Available at: https://philadelphia.cbslocal.com/2018/05/14/sentencing-day-for-edward-archer-who-shot-philadelphia-officer-jesse-hartnett-in-name-of-isis/.

CNN News, Hacker Allegedly Gave ISIS a 'Kill List' of U.S. Troops, October 16, 2015. Available at: https://edition.cnn.com/videos/us/2015/10/16/isis-hacker-malaysia-dnt-todd-tsr.cnn.

Christie, M., et al., Christmas Party May Have Triggered San Bernardino Terror Attack: Police, *ABC News*, December 1, 2016, Available at: https://abcnews.go.com/US/christmas-party-triggered-san-bernardino-terror-attack-police/story?id=43884973.

Connor, T., Texas Convert Warren Clark Sent ISIS His Resume, Report Says, *NBC News*, February 6, 2018. Available at: https://www.nbcnews.com/storyline/isis-terror/texas-convert-warren-clark-sent-isis-his-resume-report-says-n845151.

Jenny Deam, Colorado Woman's Quest for Jihad Baffles Neighbours, *LA Times*, July 25, 2014. Available at; http://www.latimes.com/nation/la-na-high-school-jihadi-20140726-story.html#page=1.

Department of Justice, Hanad Musse Pleads Guilty to Conspiracy to Provide Material Support to the Islamic State of Iraq And The Levant, September 9, 2015. Available at: https://www.justice.gov/usao-mn/pr/hanad-musse-pleads-guilty-conspiracy-provide-material-support-islamic-state-iraq-and.

Department of Justice, Maryland Man Sentenced to 20 Years in Prison for Providing Material Support to ISIS and Terrorism Financing, March 30, 2018. Available at: https://www.justice.gov/opa/pr/maryland-man-sentenced-20-years-prison-providing-material-support-isis-and-terrorism.

Department of Justice, Virginia Man Sentenced to 11 Years in Prison for Attempting to Provide Material Support to ISIL, February 24, 2017. Available at:

https://www.justice.gov/opa/pr/virginia-man-sentenced-11-years-prison-attempting-provide-material-support-isil.

Diedrich, J., A Cudahy Woman Charged with Promoting ISIS and Suggesting Attacks on Festivals, Churches Held on Bail, *Milwaukee Journal Sentinel*, June 15, 2018. Available at: https://eu.jsonline.com/story/news/crime/2018/06/15/cudahy-mom-charged-promoting-isis-attacks-held-without-bail/702851002/.

Eckel, M., and Maruf, H., "Why He Chose to Leave This Good Land?", *Voice of America*, [No Date]. Available at: https://projects.voanews.com/isis-recruit-somali-americans/.

Edgemon, E. Alabama Student Pleads Guilty in ISIS Plot, Obtaining Bomb Making Materials, *AL,* March 8, 2018. Available at: https://www.al.com/news/birmingham/2018/03/alabama_student_pleads_guilty.html.

Elgot, J,. May and Macron Plan Joint Crackdown on Online Terror, *The Guardian*, June 12, 2017. Available at: https://www.theguardian.com/politics/2017/jun/12/may-macron-online-terror-radicalisation.

Engel, R., How a North Carolina Native Ended Up on a Quest to Join ISIS, *NBC News*, September 3, 2014. Available at: https://highered.nbclearn.com/portal/site/HigherEd/flatview?cuecard=71348.

Engel, R., Plesser, B., and Connor, T., American ISIS Defector: 'I've Let My Nation Down', May 22, 2016. Available at: https://www.nbcnews.com/storyline/isis-uncovered/american-isis-defector-i-ve-let-my-nation-down-n578216.

Engel, R., Plesser, B., and Connor, T., An American ISIS Cell: The Story of 3 U.S. Recruits, *NBC News*, May 19, 2016. Available at: https://www.nbcnews.com/storyline/isis-uncovered/american-isis-cell-story-3-u-s-recruits-n573831.

Engel R., et al, The Americans: 15 Who Left the US to Join ISIS, *NBC News*, May 15, 2016. Available at: https://www.nbcnews.com/storyline/isis-uncovered/americans-15-who-left-united-states-join-isis-n573611.

Everett, R., Before Joining ISIS in Syria, Jersey Shore Man Was a Shy 'Closed Person', *NJ.com*, January 20, 2018. Available at: https://www.nj.com/atlantic/index.ssf/2018/01/nj_man_who_became_isis_commander_was_shy_closed_pe.html.

Farber, M., The Percentage of Americans Without Bank Accounts Is Declining, *Fortune*, September 8, 2016. Available at: https://fortune.com/2016/09/08/unbanked-americans-fdic/.

Goldman, A., An American Family Saved Their Son from Joining the Islamic State, Now He Might Go to Prison, *Washington Post*, 6 Sept 2016. Available at: https://www.washingtonpost.com/world/national-security/an-american-family-saved-their-son-from-joining-the-islamic-state-now-he-might-go-to-prison/2015/09/06/2d3d0f48-44ef-11e5-8ab4-c73967a143d3_story.html?noredirect=onandutm_term=.153ed638a96a.

Gordon, M., 'I Am Not a Bad Person,' ISIS Conspirator Says in Admitting he Murdered Elderly Neighbor, *Charlotte Observer*, July 17, 2017 Available at: https://www.charlotteobserver.com/news/local/article161716598.html.

Gordon, M., First American ISIS Convert in Custody, Justin Sullivan, to Face the Death Penalty, *Charlotte Observer*, March 18, 2016. Available at: https://www.charlotteobserver.com/news/local/crime/inside-courts-blog/article66952427.html.

Goudie, C., et al., Northwest Side Chicago Man Charged in ISIS Terror Case, *ABC News*, October 19, 2018. Available at: https://abc7chicago.com/northwest-side-man-charged-in-isis-terror-case/4519089/.

Gounley, T., Neighbors Never Saw Her. But Buffalo Woman Arrested by FBI was "Well Known…in the ISIS Twitter Scene, *Springfield News Leader*, February 25, 2016. Available at: https://eu.news-leader.com/story/news/crime/2016/02/25/safya-roe-yassin-well-known-isis-twitter-scene-fbi-arrested-buffalo-missouri-terrorism-woman/80621154/.

Green, E., How Two Mississippi College Students Fell in Love and Decided to Join a Terrorist Group, *The Atlantic*, May 1, 2017. Available at: https://www.theatlantic.com/politics/archive/2017/05/mississippi-young-dakhlalla/524751/;

Greenberg, T., and McCrone, B., 'I Hate You, Americans': Co-Worker, Friend Recall ISIS 'Senior Command' From Jersey Shore, *NBC News*, January 18, 2018. Available at: https://www.nbcphiladelphia.com/news/local/I-Hate-You-Americans-Co-Worker-Friend-Recalls-ISIS-Senior-Commander-From-Jersey-Shore--470009243.html.

Hall, E., Gone Girl: An Interview with An American in ISIS, *Buzzfeed News*, April 17, 2015. Available at: https://www.buzzfeednews.com/article/ellievhall/gone-girl-an-interview-with-an-american-in-isis.

Hall, E., How One Young Woman Went From Fundamentalist Christian to ISIS Bride, *Buzzfeed News*, July 20, 2015. Available at: https://www.buzzfeednews.com/article/ellievhall/woman-journey-from-chattanooga-to-isis.

Horn, D., The Terrorist Recruiter in Your Living Room, *Cincinnati*, January 18, 2015. Available at: https://eu.cincinnati.com/story/news/2015/01/17/terrorist-recruiter-living-room/21918469/.

McEnroe, P., St Paul Woman Charged with Stealing Passport to Travel to Syria, *Star Tribune*, December 3, 2014. Available at: http://www.startribune.com/st-paul-woman-charged-with-stealing-passport-to-travel-to-syria/284520161/.

Ibrahim, M., and Yuen, L., In Court Filings, ISIS Recruit Details Path from Minnesota to Syria, *MPR News*, June 11, 2015. Available at: https://www.mprnews.org/story/2015/06/11/mohamed-farah.

Jackson, J. Terror Suspect Called a Quiet Loner, Wall Street Journal, February 27, 2015, Available at: https://www.wsj.com/articles/terror-suspect-called-a-quiet-loner-1425089215.

Know Your Meme: Keep Calm and Carry On. Available at: https://knowyourmeme.com/memes/keep-calm-and-carry-on.

Know Your Meme: North by Northwest. Available at: https://knowyourmeme.com/photos/1452448-bertstrips.

Koerner, B.I., Can You Turn a Terrorist Back into a Citizen? *Wired*, Jan 24, 2017. Access via: https://www.wired.com/2017/01/can-you-turn-terrorist-back-into-citizen/.

Levine, M., Ahead of 9/11 Anniversary, FBI Arrests Kentucky Woman for Allegedly Promoting ISIS-Inspired Attacks, *ABC News*, September 9, 2016. Available at: https://abcnews.go.com/US/abc-ahead-911-anniversary-fbi-arrests-kentucky-woman/story?id=41975069.

Lipscomb, J., How Harlem Suarez Went From Cuban Immigrant to Wannabe ISIS Jihadi, *Miami New Times*, September 3, 2017. Available at: https://www.miaminewtimes.com/news/harlem-suarez-goes-from-cuban-immigrant-to-wannabe-isis-jihadi-9643881.

Matza, M., Shooter in Philly Cop's Ambush Said he did it for ISIS, but Friends, Relatives Wonder, *The Inquirer*, February 8, 2016. Available at: http://www.philly.com/philly/news/20160208_Shooter_in_Philly_cop_s_ambush_said_he_did_it_for_ISIS__but_friends__relatives_wonder.html.

McCoy, C., Purcell, D., and Hefler, J., From Atlantic City High to ISIS: The Path of a Homegrown Terrorist, *Philadelphia Inquirer*, January 19, 2018. Available at: http://www2.philly.com/philly/news/nation_world/american-isis-commander-atlantic-city-margate-zulfi-hoxha-2-20180119.html.

McGoogan, C., FBI Director Says Companies Should Ditch Encryption, *Wired*, December

10, 2015. Available at: https://www.wired.co.uk/article/fbi-director-calls-for-encryption-end.

Mansur Mirovalev and Eric Levenson, NY Terror Suspect Planned to Return to Uzbekistan, Sister Says, *CNN*, November 5, 2017. Available at: https://edition.cnn.com/2017/11/04/us/ny-terror-attack-suspect-sister/index.html.

Monks, M., Friend Who Photographed Her Surprised by Maysville Woman's Arrest, *River City News*, September 18, 2016. Available at: https://www.rcnky.com/articles/2016/09/18/friend-who-photographed-her-surprised-maysville-womans-arrest.

Montemayor, M., Feds Have at Least Six Open Cases Looking at ISIS Support in Minnesota, *Star Tribune*, September 9, 2017. Access via: http://www.startribune.com/on-vacation-in-morocco-normandale-student-made-break-for-isis/443462893/.

Moriarty, T., How Brendan Tevlin's Murder Case is an Example of a New Kind of Terror, *NJ.com*, May 14 2019. Available at: https://www.nj.com/essex/2018/04/brendan_tevlin_killing_reflects_terror_threat_expe.html.

Mueller, B., New Jersey Man Pleads Guilty to Pledging to Join ISIS, *New York Times*, September 9, 2015 Available at: https://www.nytimes.com/2015/09/10/nyregion/new-jersey-man-pleads-guilty-to-pledging-to-join-isis.html.

NBC News, EXCLUSIVE: American Extremist Reveals His Quest to Join ISIS, September 3, 2014. Available at: https://www.nbcnews.com/storyline/isis-terror/exclusive-american-extremist-reveals-his-quest-join-isis-n194796.

New York Timed Editorial Board, The New Radicalization of the Internet, *New York Times*, November 24, 2018. Available at: https://www.nytimes.com/2018/11/24/opinion/sunday/facebook-twitter-terrorism-extremism.html.

Pelley, S., In God's Name, *CBS Sixty Minutes*, October 30, 2016. Available at: https://www.cbsnews.com/news/60-minutes-american-teen-isis-cell-leader-scott-pelley/.

Perry, K., and Brennan, P., Father: Terror Plot Suspect Was A 'Momma's Boy', *Cincinnati.com*, January 23, 2015. Available at: https://eu.cincinnati.com/story/news/crime/crime-and-courts/2015/01/14/fbi-cincinnati-man-plotting-us-capitol-attack-arrested/21770815/.

Roebuck, J., Facing Sentencing, N. Philly Mom Married to Islamic State Soldier is No Aberration, *The Enquirer*, September 4, 2017. Available at: http://www.philly.com/philly/news/pennsylvania/philadelphia/facing-sentencing-n-philly-mom-married-to-isis-soldier-is-no-aberration-20170905.html.

Roebuck, J., North Philly Woman Gets 8 Year Term for Plan to Leave Kids, Marry IS Soldier, *The Inquirer*, September 6, 2017. Available at: http://www.philly.com/philly/news/pennsylvania/philadelphia/north-philly-mom-gets-8-year-term-for-plan-to-leave-kids-marry-isis-soldier-20170906.html.

Sewel, D., Attorneys: Tri-State Man Behind Terror Plot Now Rejects "Radical Islam" Wants Lighter Sentence, *WPCO Cincinnati*, November 30, 2016. Available at: https://www.wcpo.com/news/local-news/hamilton-county/cincinnati/defense-urges-lighter-sentence-for-plot-to-attack-us-capitol.

Schwartz, R., and Kreider, R., Online Chatter After NYC Terror Arrests: 'Delete Her From Your Phone', *ABC News*, April 6, 2015. Available at: https://abcnews.go.com/International/online-chatter-nyc-terror-arrests-delete-phone/story?id=30124247.

Shapiro, E., Philadelphia Police Office Shot By Alleged Islamic Extremist, *ABC News*, January 8, 2016. Available at: https://abcnews.go.com/US/man-accused-shooting-philly-cop-confessed-committing-act/story?id=36169588.

Shapiro, E., et al., Ohio State University Student Dead After Driving Into Crowd, Stabbing People at OSU Campus, *ABC News*, November 28, 2016, Available at: https://abcnews.go.com/US/ohio-state-university-student-dead-driving-crowd-stabbing/story?id=43821371.

Shoichet., C. and Pearson, M., Garland, Texas, Shooting Suspect Linked Himself to ISIS in Tweets, *CNN*, May 5, 2015. Available at: https://edition.cnn.com/2015/05/04/us/garland-mohammed-drawing-contest-shooting/index.html.

Siddique, H., and Grierson, J. Home Office Proposes Offence of Possessing Terrorist Propaganda, *The Guardian*, January 14, 2020. Available at: https://www.theguardian.com/uk-news/2020/jan/14/home-office-proposes-offence-of-possessing-terrorist-propaganda?CMP=share_btn_tw.

Smith, M., and Goldberg, A., From Somalia to US: Ohio State Attacker's Path to Violence, *New York Times,* December 1, 2016. Available at: https://www.nytimes.com/2016/12/01/us/from-somalia-to-us-ohio-state-attackers-path-to-violence.html.

Snell, R., FBI Hunts Doctor from Flint Area Tied to Islamic State, *The Detroit News,* June 23 2016. Available at: https://eu.detroitnews.com/story/news/local/michigan/2016/06/23/fbi-hunts-doctor-flint-area-tied-islamic-state/86270418/.

Sullivan, K., and Wan, W., Troubled. Quiet. Macho. Angry. The volatile life of the Orlando shooter. *The Washington Post*, June 17, 2016. Available at: https://www.washingtonpost.com/national/troubled-quiet-macho-angry-the-volatile-life-of-omar-mateen/2016/06/17/15229250-34a6-11e6-8758-d58e76e11b12_story.html?utm_term=.2d7ee59892e0.

Susman, S., Islamic State Presence in the U.S. is 'the New Normal,' FBI Director Says, *LA Times*, November 19, 2015. Available at: https://www.latimes.com/nation/la-na-isis-us-20151120-story.html.

Stack, L., Wisconsin Woman Used Hacked Facebook Accounts to Recruit for ISIS, Prosecutors Say, *New York Times*, April 22, 2019. Available at: https://www.nytimes.com/2019/04/22/us/wisconsin-woman-isis.html.

St Louis Post Dispatch, Rockford Woman Pleads Guilty in St Louis Terrorist Funding Case, *Chicago Tribune*, 29 Sept, 2015. Available at: http://www.chicagotribune.com/news/local/breaking/ct-rockford-woman-terrorist-funding-case-20150929-story.html.

Temple-Raston, D., He Wanted Jihad. He Got Foucault, *New York Magazine,* November 27, 2015. Available at: http://nymag.com/intelligencer/2017/11/abdullahi-yusuf-isis-syria.html?gtm=bottom.

Washington Post Editorial Board, Beware the Rabbit Hole of Radicalization, August 6, 2019. Available at: https://www.washingtonpost.com/opinions/beware-the-rabbit-hole-of-radicalization/2019/08/06/0d589a96-b7bc-11e9-a091-6a96e67d9cce_story.html.

Wassef, M., Facing 100-year sentence, Staten Islander Details his 'misguided' Transformation from Kind Child to ISIS Backer, *SI Live*, April 25, 2018. Available at: https://www.silive.com/news/2018/04/staten_island_terrorist_faces.html.

Wilkinson, A., We Need to Talk About the Online Radicalisation of Young, White Men, *The Guardian,* November 15, 2016, Available at: https://www.theguardian.com/commentisfree/2016/nov/15/alt-right-manosphere-mainstream-politics-breitbart.

Williams, P., and Abdullah, H., FBI: San Bernardino Shooters Radicalized Before They Met, *NBC News*, December 9, 2015. Available at: https://www.nbcnews.com/storyline/san-bernardino-shooting/fbi-san-bernardino-shooters-radicalized-they-met-n476971

Wood, G., An American Climbing the Ranks of ISIS, *The Atlantic*, January 25, 2017. Available at: https://www.theatlantic.com/magazine/archive/2017/03/the-american-leader-in-the-islamic-state/510872/.

Yuen, L., Gone to Syria: Family Fears Woman Latest Minnesotan Drawn to War-torn Region, *MPR News*, September 11, 2014. Available at: https://www.mprnews.org/story/2014/09/11/muslim-woman-disappears-syria.

Zakaria, R., The Law Needs to Catch Up with the Reality of Domestic Terrorism, *CNN*, October 29, 2018. Available at: https://edition.cnn.com/2018/10/29/opinions/domestic-terrorism-legal-limitations-rafia-zakaria/index.html.

Zavadski, K., His Mom and Dad Hid a Terrible ISIS Secret, *The Daily Beast*, January 17, 2017. Available at: https://www.thedailybeast.com/mom-and-dad-hid-a-terrible-isis-secret.

Zavadski, K., The American Anti-Vaccine Mom Turned ISIS Superstar, *The Daily Beast*, March 29, 2016. Available at: https://www.thedailybeast.com/the-american-anti-vaccine-mom-turned-isis-superstar.

Acknowledgements

Every PhD student is aware that completing their thesis is not a solo project. I have been lucky to have four incredible supervisors who have guided me through this process – Prof. Stuart Macdonald, Prof. Edwin Bakker, Dr Lella Nouri, and Dr Alastair Reed. Lella, you've been there for me daily and have helped steer me through. Alastair, as well as your PhD guidance, you welcomed me when I moved to the Netherlands and have been a constant source of sanity throughout. Stuart, thank you for your calm (and patient!) advice, both as part of the PhD but also for my professional development over these years. Edwin, your help, particularly towards the end, was very valuable and I appreciate it.

The support network for a PhD student goes beyond the supervisory team, and I am fortunate enough to call two universities home. Thank you to everyone in both the Law School and Criminology Department at Swansea University. I'd also like to think everyone at ISGA at Leiden University; the summer I spent in Den Haag was incredibly rewarding and I'm grateful for both the academic and personal support.

I am particularly grateful to my teammates at CYTREC throughout the years: Sara, Amy-Lou, Lizz, Seán, Katy, Patrick, Ninian, Maura, Kamil, David, Simon, Sam, Kris, Reza, Huw, Nnenna, Nuria and everyone else. Working as part of such a wide network of talented people has been extremely helpful in progressing as a scholar. I'm also thankful for the wider PGR community at Swansea – Joe, Jordan, Phatsi, Simon, Aaron et al. We all had some stressful, but fun, times in that room and supported each other.

I am also lucky to be part of an inclusive and friendly community of researchers. When in the Netherlands, I spent time working with the great team at the ICCT, which is where I first met Haroro Ingram, Craig Whiteside, J.M. Berger, Sergei Boeke, and Donald Holbrook. I'm also thankful for the team of scholars at George Washington University's Program on Extremism – I drew heavily from their repository to collect the data for this project and everyone on the team was helpful and kind whenever we met. I'd like to thank Audrey and Bennett in particular, who were great conference companions over the last 5 years. Similarly, when I asked Paul Gill many years ago about the best way to research online radicalisation empirically, his helpful advice led to the foundations of this project.

I need to thank my loved ones for their support over the last 5 years. Mum, Dad, Chris, Helen, Cat, Luke, Leticia, Eliana, Amelia, and Jem – your love and care has been invaluable and helped me get through the rough times. Regular trips to see friends in Cambridge, London, or Sheffield have provided important sanity-breaks and much-needed opportunities to blow off steam too; there are too many names to list everyone but thank you! Finally, Cath, and Ella, you make each day brighter than the last and spending time with you makes all the weekend work and late nights worth it.

Curriculum Vitae

Joe Whittaker was born in Cambridge (United Kingdom) on 20 December 1988, attending Mayfield Primary School, Impington Village College, and Hills Road Sixth Form College. He achieved a first-class degree in Politics & Philosophy BA from the University of Hull in 2014 and a MA with distinction in International Politics from the same institution in 2015. For the latter he was awarded the Parekh Prize.

In 2016, he began a joint PhD studying "online radicalisation" with Swansea University in Wales and Universiteit Leiden in the Netherlands. During this time, he undertook several research and teaching assistant positions. He also spent the summer of 2017 working with the International Centre for Counter-Terrorism in the Hague, where he remains a research fellow. He also won a travel bursary to work with the CVE think tank Hedayah in 2018. Joe is currently a member of the Global Internet Forum to Counter-Terrorism's "Content-Sharing Algorithms, Processes, and Positive Interventions" working group.

After completion of his PhD, Joe is looking ahead to future work involving the role of recommendation algorithms in the amplification of extreme content on social media.