# Online Radicalisation: Moving Beyond a Simple Dichotomy

Chamin Herath[1] and Joe Whittaker[2]

**Abstract**

Online radicalisation to terrorism has become a pervasive policy concern over the last decade. However, as a concept it lacks clarity and empirical support. In this article, we add an empirical and theoretical lens to this problem by analysing the trajectories of 231 Islamic State terrorists. We use cluster analyses to create typologies of individuals' different online and offline antecedent behaviours, including the ways in which they engaged in networks with co-ideologues and how they prepared for their events. The findings suggest four types of pathway within our dataset: 1) The 'Integrated' pathway which has high network engagement both online and offline, mostly made up of individuals that plotted as part of a group; 2) The 'Encouraged' pathway contains individuals that acted more in the online domain at the expense of offline; 3) Terrorists in the 'Isolated' pathway are defined by a lack of interaction across either domain; 4) The 'Enclosed pathway encompassed actors that displayed greater offline network activity, but still utilised the Internet for planning their activity. These typologies help to move beyond the dichotomy of online or offline radicalisation; there remain few individuals that either exclusively use the Internet or do not use it at all. Rather, we can conceptualise Internet usage on a spectrum in which these four typologies all sit.

**Keywords**
Terrorism; Extremism; Online Radicalisation; Radicalisation

## Introduction

With currently over 4.83 billion users worldwide (Internet World Statistics, 2020), the Internet has transformed modern life. However, along with the benefits of communications, video content, and smart phones, a range of security concerns have arisen. Terrorists have frequently been noted as early adopters of the Internet (Levin, 2015; UN CTED, 2015), using online fora, chat rooms, websites, and email in the Web's early days (Sageman, 2008a). More recently, the so-called Islamic State (hence IS) have utilised the web to conduct sophisticated online recruitment and propaganda campaigns (Klausen, 2015; Winter, 2015; Zelin, 2015; Ingram, 2016). The group achieved remarkable success: over 50,000 foreign fighters travelled from countries around the world to join IS (Cook and Vale, 2019) and dozens of attacks were conducted by terrorists that were directed or inspired by the group. This includes the Paris attack of 2015 (Castillo *et al*., 2015).; the Orlando Pulse Nightclub shooting in 2016 (Tsukayama *et al*., 2016); and the Manchester Arena bombing (BBC, 2017). It therefore seems logical to ascribe these successes to the group's wide-reaching online propaganda and recruitment campaigns. As a result, the Internet has been perceived as a significant, or even causal, part of the trajectories of contemporary terrorists – "online radicalisation." Following the aforementioned attack in Orlando, FBI director James Comey noted that the attacker had "radicalized, at least in some part, through the Internet" (Pilkington & Roberts, 2016). In 2017, former UK Prime Minister Theresa May and French President Emmanuel Macron responded to the threat posed by terrorists' use of the Internet by establishing a joint campaign to tackle online radicalisation (HM Government, 2017).

In this paper we question and dissect the concept of online radicalisation using an empirical dataset of 231 US-based IS terrorists. To do this, we perform a cluster analysis to explore patterns in

[1] Cyber Research Analyst at the Royal United Services Institute (RUSI)
[2] Lecturer in Cyber Threats at Swansea University, Department of Criminology.

behaviours which are grouped into different terrorist pathways. These groups are subsequently turned into Webarian "ideal-types" which help to explain the different levels of Internet usage. We find four types of pathways, which all demonstrate the intertwined nature of online and offline behaviours; even though some terrorists use the Internet more than others, each of these categories exist on a spectrum, rather than the binary online/offline distinction in which it is often discussed. The findings offer an important policy contribution – responses are often fixated on a particular domain, but this research shows that a multiplicity of interventions must be utilised using both online and offline tactics.

**Online Radicalisation**

The concept of online radicalisation pre-dates the rise of IS by several years. As early as 2008, eminent terrorism scholar Marc Sageman argued that the Internet had completely altered the nature of radicalisation. In particular, he argued that there were certain salient features that existed online that did not offline, including people acting more vitriolic, group polarisation due to easier exit ramps, and non-hierarchical structures (Sageman, 2008a). He even went as far as to argue that 'face-to-face radicalization has been replaced by online radicalization' (Sageman, 2008b, p. 41). Other scholars have mirrored Sageman's thoughts; Gabriel Weimann argues that offline networks had been outstripped in importance by online ones and '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). The idea of a "lone wolf" radicalising with co-ideologues online, free from the constraints of physical terrorist organisations has been posited by other scholars in the field (Anti-Defamation League, 2014; Post, McGinnis and Moody, 2014). However, as we will show below, the empirical research on this topic is far more equivocal on the role of the Internet.

As a concept, it is not entirely clear what "online radicalisation" constitutes. Gill and colleagues note that there is an abundance of conceptual problems associated with the phrase:

> 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)

Conducting an academic literature search, Macdonald and Whittaker (2019) find that only 21% of studies on this topic define what online radicalisation means and those that do define it can have substantially different understandings. Von Behr and colleagues conducted a literature review which led to them towards five hypotheses of online radicalisation:

1. The internet creates more opportunities to become radicalised.
2. The internet acts as an 'echo chamber'.
3. The internet accelerates the process of radicalisation.
4. The internet allows radicalisation to occur without physical contact.
5. The internet increases opportunities for self-radicalisation. (von Behr *et al.*, 2013)

Some research conceptualises the process as terrorists or extremists that act online (i.e. Von Behr and colleague's fourth hypothesis) without any face-to-face contact (Sageman, 2008a; Anti-Defamation League, 2014), while other studies focus more on the effects of the Internet:

> 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 short, the process is often not explicitly defined and can mean several different things. Conducting a literature review on the topic, Meleagrou-Hitchens and Kaderbhai aruge 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).

There is good reason to question the conceptual utility online radicalisation. Macdonald and Whittaker (2019) argue that the most problematic aspect of the phrase may be the implied demarcation between the online and offline realms. Maura Conway notes that several commentators contrast online interactions with offline ones, which privileges "real world" activity and understates the social aspect 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. It is precisely the functionalities of the social Web that causes many scholars, policymakers, and others to believe that the Internet is playing a significant role in contemporary radicalization processes (Conway, 2017, p. 80).

This speaks to a wider debate within Internet Studies on the conceptualisation of the Internet. Jurgenson (2012) highlights two key perspectives that are relevant here. On one hand, "digital dualism" in which the Internet is a revolutionary new space free from offline limitation and social structures. This perspective speaks to the view of the Internet as the new "Wild West" where users can say and do whatever they please without consequence or accountability in the so-called 'real world' (Davis, 2006; Fitch, 2009) On the other hand is the "augumented reality" perspective in which the online and offline domain are deeply enmeshed. On this reading, Internet-based devices such as phones and laptops, as well as non-physical applications such as websites and social media platforms are "digital prostheses" which are no more than extensions of the offline or physical embodiment of an individual (Rey & Boesel, 2014, p.178).

**Previous Research**

Although there has been a growth of empirical research on the topic of terrorists use of the Internet, there is still a dearth of data-driven studies which analyse terrorists' behaviours. The field tends to over-rely on the "supply-side", which is to say, research which analyses content such as e-magazines (Ingram, 2018; Macdonald and Lorenzo-Dus, 2019), pictures (Huey, 2015; Zelin, 2015), and videos (Winter, 2015; Nanninga, 2019), or social media analyses of supporters of terrorism (Berger and Morgan, 2015; Clifford and Powell, 2019; Fisher, Prucha and Winterbotham, 2019). While it is important to understand the online environments in which terrorists inhabit, this has come at the expense of the "demand" side – how terrorists actually use the Internet. An over-reliance on the media that terrorists *could* interact with often suggests a degree of causality about how terrorists will perceive it, which cannot be proven or falsified (von Behr *et al.*, 2013). Scholars have highlighted that there is a paucity of empirically valid research into how the Internet impacts pathways towards terrorism (Gill *et al.*, 2017; Macdonald and Whittaker, 2019).

In the absence of data-driven studies, a significant portion of academics, practitioners and policymakers have turned to the concept of 'online radicalisation' to emphasise the role of the Internet as a 'key radicaliser' in contemporary terrorist trajectories. As a result, the issue of 'online

radicalisation' has been regarded as one of today's most pressing security challenges (Macdonald and Whittaker by several governing bodies across the globe (OSCE, 2013; Council of the European Union, 2014; European Commission, 2015; Europol, 2016). However, much of this is based off anecdotal evidence and unsubstantiated claims; in an extensive literature search using the term, Gill and colleagues discovered that out of a total of 200 studies identified, 6.5% had used data in some form, thus suggesting that inferences made from the vast majority of the literature using the term are not supported empirically (Gill *et al.*, 2015).

In recent years there have been a handful of studies which have sought to analyse the role of the Internet in pathways towards terrorism. These studies suggest that the Internet is used widely by terrorists. For example, Bastug, Douai and Akca (2018) analyse the Internet usage of 51 Canadian travellers to IS, finding that social media played a role – either during or after their radicalisation – for 76% of their sample for whom data could be found. Similarly, Jensen *et al.* (2018) examined the social media usage of 478 US-based extremists from 2005-2016, finding that the Internet had become more important as time progressed; from 2005-2010, only around a quarter used social media and they only deemed it a primary cause of radicalisation in 1% of cases. However, from 2011-2016 this rose to 76% using it, and estimating it to be of primary importance in 17% of cases. In the years 2015 and 2016 alone, they find that around 85% of actors used social media. This is in concurrence with Gill and Corner's (2015) study on 119 UK and US-based lone actor terrorists, who find that the use of the Internet has risen over their sample of 1995-2015.

However, when analysing the role of the Internet compared to other factors, the importance of the Internet is often reduced. Von Behr *et al.* (2013) test five hypotheses of "online radicalisation" in 15 cases of UK-based terrorists and extremists using both interview techniques and computer data. They found a digital footprint in all their cases, supporting the hypothesis that the Internet increases opportunities to become radicalised, and the majority of their cases suggested that the Internet acted as an echo chamber. However, they find little evidence to suggest that the Internet had replaced the need for physical face-to-face contact; that it accelerates the process of radicalisation; or that it increases opportunities for "self-radicalisation". Other small sample qualitative studies have also suggested that the Internet plays an important role in terrorism. Both Koehler (2014) and Gaudette, Scrivens and Venkatesh (2020) conducted interview research with 8 and 10 former far-right extremists, respectively. Both pieces of research find that the Internet played a key role in their participants' pathways and played an important part in ideological development and advancement, with multiple participants stating that they were drawn to the movement via the Internet. However, both also highlight the intertwined nature of the online and offline domains: 'the Internet is not a structure separated from the 'real world' but dynamically connected with it' (Koehler, 2014, p. 128).

There have been several studies with a larger sample size that have sought to investigate the role of the Internet. One of the most important contributions to the existing literature on the subject comes from Gill *et al.* (2017) which utilises open-source data to analyse the online and offline behaviours of 223 UK-based terrorist offenders. They find that antecedent terrorist behaviours were compartmentalised across both the online and offline domains and argue that an online/offline dichotomy may be a false one. In a study that analysed the pathways of 137 convicted French jihadists, Hecker (2018) found that while the Internet had been used to plan, communicate with likeminded individuals, and access propaganda, there was no evidence to suggest that actors had 'radicalised' entirely online. Reynolds and Hafez (2017) test three hypotheses to explain the mobilisation of 99 German foreign fighters, finding that offline peer-to-peer networks was a more likely explanation than online radicalisation or a lack of social integration. Baugut and Neumann

(2019) researched the use of propaganda by Islamists in Germany and Austria. Although the Internet was used heavily to access this propaganda, the act of consuming this propaganda was also intertwined with activities in the offline domain. For example, participants reported that they watched YouTube videos in groups and discussed them together afterwards.

In previous research conducted on the same dataset, (Whittaker, 2021) analysed the online behaviours of 231 IS terrorists in the US. The study finds that 92% of terrorists use the Internet for some purpose, but that those used the Internet to either engage with co-ideologues or plan their activity online were significantly more likely to do so offline as well, further lending weight to the argument made by Gill *et al.* (2017) that separating the two domains is a false dichotomy. This is echoed other research on ISIS in America; Meleagrou-Hitchens, Hughes and Clifford (2020) challenge the notion of online radicalisation as well, suggesting that it is a misnomer when it comes to most American cases: "Radicalization processes usually derive from several reinforcing factors, the majority of which occur away from computer and mobile phone screens and involve human interactions" (Meleagrou-Hitchens, Hughes and Clifford, 2020, p. 16).

These studies present a relatively clear scholarly consensus of the role of the Internet in pathways towards terrorism. At first glance, it is apparent that terrorists use the Internet in high numbers for a range of antecedent behaviours. In fact, research conducted in a more recent timeframe suggests that the use of the Internet may be increasing (Gill *et al.*, 2017; Bastug, Douai and Akca, 2018; Whittaker 2021). However, these pieces of research show that the Internet is not a cause, but rather a facilitator of engaging in terrorist activity. Rather, there are a multiplicity of dynamics that are active across both the online and offline domain. Importantly, this suggests that there may be a false dichotomy. However, there is still a paucity of data-driven research on this topic, so all current conclusions must be tentative.

**Methods**

This research seeks to add to the data-driven studies mentioned above which have found that terrorist behaviours are intertwined between the online and offline domain. These studies have tended to focus on the differences in experiences between those that use the Internet and those that do not. For example, both Gill *et al.* (2017) and Whittaker (2021) examine whether those that use the Internet to network with co-ideologues are more likely to also do so offline. This study seeks to build on this by using a cluster analysis to categorise terrorist actors by their online and offline behaviours to create typologies to help explain different levels of reliance on the Internet.

*Radicalisation*

The term "radicalisation" is contested within the academic literature and is often deployed to mean the process of towards three different ends points: terrorism (Moghaddam, 2005; Silber & Bhatt, 2007; Klausen et al., 2016), extremism (McCauley & Moskalenko 2008; Helfstein, 2012) or radicalism (Snow & Cross 2011; Bartlett & Miller 2012). At the heart of this debate is whether radicalisation is a process which ends with the adoption of extreme beliefs *or* extreme behaviour (Neumann 2013). Several scholars have suggested that this ambiguity should make us reconsider the use of this word (Sedgwick 2010; Borum, 2011; Schuurman & Taylor 2018). However, given that this research seeks to better understand "online radicalisation," a working definition is in order. As such, we utilise a behavioural definition: 'the process of engaging in terrorism or violent extremist actions (Borum, 2011). This does not downplay the role of ideology in the process, but rather requires the end point to be behavioural rather than a change in beliefs. In essence, it is a modified version of Sedgwick's

(2010) "what goes on before the bomb goes off," except we do not require violence as an end point as we include other acts such as travel, finance, or facilitating others.

*Data*

This study utilised an existing open-source database of 231 IS terrorist actors from the US, who were active between the years 2012 to 2020 – the same database used by Whittaker (2021). To begin, a directory of terrorist actors was created from three sources. Firstly, George Washington University Program on Extremism's ISIS Repository, holds case files of over 205 (at the time of data collection) individuals charged with crimes relating to IS (Program on Extremism, nd). Secondly, by consulting two reports on the known travellers from the US to jihadist groups in both Iraq and Syria (Meleagrou-Hitchens, Hughes and Clifford, 2018) and other parts of the world (Hughes, Blackburn and Mines, 2019). These reports, also written by researches at the Program on Extremism, identify include 64 and 36 travellers respectively. Many of these individuals have crossover with the repository, such as Abdi Nur, who was charged by prosecutors having travelled to the caliphate. However, there are several unique names in these two reports. Finally, we conduct a search on the Global Terrorism Database to identify IS-based attacks in the US from 2010-2018 (START, nd). However, 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, we searched for *all* incidents of terrorism over the period. Because the GTD labels incidents of terrorism rather than individual actors, if an attack had multiple terrorists, an individual entry was made in the directory. In total, the GTD search led to 365 entries, meaning the directory has 670 terrorists before amending duplicate names such as Nur, leaving a sample 637 unique names.

Once the directory had been compiled, data were collected from several types of open-sources. To begin, court documents were searched for via the Program on Extremism repository, which holds over 20,000 pages of criminal complaints, indictments, affidavits, and courtroom transcripts (Program on Extremism, nd). This was supplemented by searching for court documents via legal search engines such as CourtListener. Next, academic and grey literature which detailed terrrorist case studies were consulted (Alexander, 2016; Klausen, 2016a, 2016b; Klausen *et al.*, 2016, 2018; Clifford and Hughes, 2018). After this, searches for journalistic sources were conducted using the LexisNexus archive, Google News. Finally, it was cross-referenced with the Counter-Extremism Project's 'Terrorists and Extremists Database' (Counter Extremism Project, nd). Collecting data from multiple sources is important because an over-reliance on a single type of source can lead to selectivity bias and therefore produce unstable results (Chermak *et al.*, 2012; Behlendorf, Belur and Kumar, 2016).

A range of inclusion and exclusion criteria were applied after data collection – a flowchart for this process can be seen in the appendix. To begin, a minority of cases had insufficient data to make a firm analysis. Where no antecedent and no event behaviours could be found, cases were excluded from the sample. This mostly relates to listed travellers in the report by Meleagrou-Hitchens, Hughes and Clifford (2018), but for whom more information was not available. An example of this is Mamadou Bah, who is name as an individual who joined IS in the report, but for whom no other information can be found.

Next, we consider whether individuals should be considered part of the Islamic State. This presents a problem because the contemporary terrorism landscape is ambiguous with regards to membership. Although there have been instances of the group directing attacks by its members, the majority of cases represent smaller cells or lone actors who have varied links to the organisation but are inspired

to act on its behalf (Whittaker 2019). Therefore, we draw from START's Profiles of Individual Radicalisation in the United States (PIRUS) Codebook, who define membership to a group broadly, even if the group does not acknowledge membership (START, 2018). In this case, actors that either explicitly support the group or consume its ideological materials they are deemed to be part of the group, but only if their actions are deemed to be in furtherance of the group's goals. For example, for those that travelled to the caliphate, to be included there needed to be positive evidence that they supported the group and were not coerced.

Next, we had to decide how to deem someone a "terrorist." There is a long debate within terrorism studies regarding the definition of terrorism (Ganor, 2002; Schmid, 2004; Ramsay, 2015), and it is a central thesis of critical terrorism studies that states' "defining agency" is problematic because of their focus on non-state actors (Stohl, 2008). Given that the research is focused on terrorism in the US, it makes logical sense to utilise the definition set out in their law and include individuals charged with terror-related offences. However, many individuals in the US are charged with other crimes because prosecutors believe they are more likely to secure a conviction (Meleagrou-Hitchens, Hughes and Clifford, 2020). These individuals are often charged with terror enhancements if the crime is deemed to be sufficiently related to terrorism (Skinner, 2015). However, this would still leave some individuals that are clearly terrorists that are not included; for example, those that died conducting their attack and were not charged. Therefore, to be included, the actor must have fulfilled one of the following criteria:

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

While there is merit to critical theorists' arguments regarding the definition of terrorism, it should be noted that our first inclusion criteria already removed several "edge cases" because individuals needed to self-identify with, and act with clear ideological motivation on behalf, of a group for whom there is little debate that they are terrorist. An example of this process is the cases of Mohommad Ali and Sumaiya Ali, a married couple who lied about their sons' 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. Fundamentally, there is not an easy way to resolve this issue – there is clear merit to grounding the inclusion criteria to the criminal justice system of the country under study, but we also accept the claim that governmental definitions are politically motivated.

Furthermore, to be deemed as operating within the US, one of three following criteria must have been met:

a) Been charged in the US, or
b) Be a US Citizen or permanent resident *and* resided in the US until five years before their event, or
c) Resided in the US at the time of their activity.

Rather than set an arbitrary date range, this research is dictated by the start point of IS' activity and seeks to capture as many of their actors as possible. As a result, cases range from the earliest known date of 2012 to the end of data collection in June 2020.

At the end of data collection, eighty five percent had been formally charged (n=197), of whom 60% had pleaded guilty, 13% were found guilty at trial, and 27% of whom had not faced trial or made a plea. This leaves an ethical question with regards to inclusion given that individuals have a presumption of innocence. This issue is discussed by Whittaker (2019), who highlights the potential damage of publicly naming an individual a terrorist. On the other hand, there are clearly terrorists that have not (and will not face trial), for example Omar Mateen, the Pulse nightclub shooter, who died conducting his attack, but was publicly named as the assailant by the FBI (Tsukayama *et al*., 2016). This raises a tension between harming research participants (who have not consented to the use of their data) and conducting rigorous research. Ultimately, the potential harms to the research participants were deemed to be minimal given for two reasons: Firstly, given the nature of data collection from secondary sources, the individuals' names were already in the public domain, and secondly, the main analysis in this article is quantitative in nature and therefore the data are anonymised. Where qualitative examples are given, if an individual is still progressing through the criminal justice system, qualifying language is used to discuss their case (e.g. "allegedly" or "x is accused of…").

The inclusion and exclusion criteria were initially applied by a single author as part of his doctoral research. However, when the data were re-coded in June 2020, the coders were asked to reflect on the inclusion and exclusion criteria and no cases were deemed to be incorrectly included. However, this leaves open the possibility that some terrorists were incorrectly excluded, which we acknowledge as a limitation of the present research.

After applying the inclusion and exclusion criteria and accounting for duplicated cases, the final sample is 231 terrorist actors. This includes 187 individuals first identified in the Program on Extremism repository, 30 travellers identified in the two reports, and 14 attackers identified from the Global Terrorism Database. A random selection of 10% of these case files (n = 23), show that each case file is on average 5,600 words long (around 10 pages), with eight sources per file (an average of 2.8 criminal documents and 5.2 journalistic/academic/grey). However, the court documents were considerably richer in detail and longer, making up an average of around 3,500 words per file (63%), while the other documents made up around 2,100 words (37%)

*Codebook*

After data collection was completed, the data were coded using a codebook derived from the academic literature that has been used in previous studies which analysed the role of the Internet in terrorist pathways (Whittaker 2019). That study coded for a range of demographic, network, and event-specific variables. This included whether individuals networked with co-ideologues online or offline; whether they used the Internet to learn about or plan their intended activity (or did so offline); whether they acted alone, in a pair, or as part of a group; and their role in the event. As discussed above, this study highlighted that the online and offline domains are not easily separable, but research has yet to take the next step and explore the extent of this interaction.

The present study expands on this by adding more specific offline equivalent behaviours: While the previous study coded for whether individuals used the Internet to reinforce their beliefs; engaged in an ideological debate or sought legitimisation from a spiritual authority, this study also includes whether the individuals engaged in these behaviours offline. Fundamentally, the addition of more offline network and event-specific behaviours allowed this study to gather an equal amount of data regarding actors' online and offline experiences and, therefore, permitted it to make data-driven

inferences in relation to the extent to which the two domains interact. In total, we use 18 "network" variables, and 16 "event" variables for our analysis, which can be located in Table 1 and 2.

Coders were instructed to assess whether evidence that a certain behaviour was present or not. For example, to be coded as "Reinforced Beliefs Online", individuals may have gone online to discuss and solidify their views. An example of this would be Houcine Ghoul, who had previously demonstrated he held radical beliefs, using his workplace Internet to constantly engage with IS content which further cemented his ideological viewpoints, such as providing him with a historical justification for immolating enemies (USA v. Houcine Bechir Ghoul, 2017). As another example, to be coded as seeking legitimisation offline, one may have a mentor/mentee relationship with another individual, like Akhror Saidakhmetov, who learned from several face-to-face meetings with his co-ideologue Abdulrasul Juraboev. The former affectionately called the latter "Sheik" in tribute to his deep religious knowledge (USV v. Akhror Saidakhmetov).

For cases where there were plots with multiple conspirators, it is worth reiterating that an individual case file was created for each individual and coded according to the information that could be ascribed to each actor. Therefore, if there is evidence of two individuals in the sample speaking to each other online, this could be classified as "online contact with a network" for both, as was the case with David Wright and Zulfi Hoxha, who maintained contact via Skype and PalTalk (Hughes, Meleagrou-Hitchens, and Clifford, 2018). In plots that maintained undercover officers, network behaviours were coded as contact with co-ideologues because it was deemed more important to discern who the terrorists believe they were speaking to rather than the number of "true" terrorists.

These variables were coded dichotomously – i.e. either a '1' for 'Present' or a '0' for 'Not Present'. This follows the lead of Gill and colleagues, who argue that definitive 'Not Present' answers are a rarity in open-source research because the data are insufficiently granular; they argue that if one has access to closed-source data such as police files, then multiple imputation methods may be possible (Gill *et al.*, 2017). All else being equal, it is better to minimise assumptions around missing data as it can create misleading findings that are not reflected when these assumptions are removed (Safer-Lichtenstein, LaFree and Loughran, 2017). However, this may be beyond the reach of the richness of data available to terrorism scholars, so therefore, this research is open about the assumptions that it is making (i.e. that missing data is more likely to be "No" than "Yes").

If there were any discrepancies between these sources, a hierarchy of reliability was applied in which court documents were prioritised, followed by the academic articles and then news sources, with local reporting of trials taking precedence over national reporting (Clemmow *et al.*, 2020; Gill, 2020). On the rare occasion that sources on the same level disagreed with each other, coders decided based on the reliability of the source (e.g. tabloids were considered low-quality) and the date of the source (i.e. more recent sources were considered to be more reliable than ones written immediately after the event). However, it should be noted that disagreements were a relative rarity and where they did exist, it was usually a high-quality source, such as a court transcript, versus a lower quality newspaper article.

The data were coded by four independent raters in the summer of 2020. To begin, a training session was conducted in which the codebook and overall strategy was explained by the supervisor to the coders. A trial run was then conducted in which each rater coded the same case file independently before feeding back to the larger group to compare and discuss results. Agreement was generally high and disagreements were clarified by the supervisor. Following this, two rounds of inter-coder tests were run to establish the aggregate reliability for the variables, following the procedures of

similar terrorist database research (LaFree et al. 2018; Safer-Lichtenstein et al. 2017; Horgan et al. 2016). 20 out of the total 231 cases were tested – 10 prior to coding the data and 10 after finishing coding, which were tested for inter-coder reliability using Krippendorff's alpha, yielding an α of .675 (95% CI = 0.66 – 0.69), which is deemed acceptable to draw tentative conclusions (Krippendorff, 2004).

*Analysis*

To analyse the interactions between the online and offline domains in terrorist pathways, we conduct a two-step cluster analysis using the network and event-specific behavioural data. As a statistical method, cluster analysis is an exploratory technique (Everitt, 1993) therefore it is well-suited to the analysis of the online-offline dynamic because it helps identify undiscovered patterns within the data. It does this by grouping similar objects (e.g. the cases of terrorist actors), based on certain characteristics (e.g. their online and offline behaviours) in order to 'detect multidimensional sub-types that are embedded within the data' (Clemmow, Bouhana and Gill, 2020, p. 3). As these sub-types, or clusters, are entirely determined from the data, cluster analysis can be used as a basis for inductive theory construction, whereby new theories are developed rather than tested (Pell & Hargreaves, 2011; Whittaker and Elsayed 2019). While it is desirable for the data to be representative of the wider population of interest, exploratory analysis allows for more flexibility and open-mindedness with the aim of inductively deriving 'generalisations about the group, process, activity, or situation under study' which can be transferable in future research (Stebbins, 2001; p.5).

In prior research, cluster analysis has been used in areas such as investigative psychology and criminology to identify the different behavioural pathways of several types of sexual offenders (Proulx & Beauregard, 2014; Stefanska et al., 2015; Horan & Beauregard, 2017). More recently, it has been applied to the field of terrorism studies as a way to identify distinctive typologies of lone-actor terrorists (Clemmow *et al.*, 2020; Clemmow, Bouhana and Gill, 2020). Much like the abovementioned studies, this study opted for two-step clustering over k-means and hierarchal clustering for two main reasons. Firstly, as the best number of clusters within the data was unknown, k-means cluster analysis was deemed to have been impractical as a key requirement of using this clustering technique was to know the optimum number of clusters than can be found within the data. Secondly, while hierarchical cluster analysis identifies the best number of clusters, two step-cluster analysis was favoured because the hierarchical clustering technique is more sensitive to order effects, or the order in which the variables are imputed (IBM, 2020).

As suggested by its name, a two-step cluster analysis follows a two-step procedure. In the first step, the cases are grouped into pre-clusters based on a likelihood distance measure. As the data were categorical (i.e. they were coded into different categories), this study used the log-likelihood distance measure (Norusis, 2011). By pre-clustering the cases before determining the optimum number of clusters, much larger datasets can be analysed in a shorter amount of time (Bacher, Wenzig, & Vogler, 2004). In the second step, a hierarchical clustering algorithm is run to determine the maximum number of clusters. Once the maximum number of clusters have been identified, the quality of the proposed cluster solution is scored based on a silhouette measure of cohesion and separation, which is measured on a scale between -1 and +1. If the score is closer to +1 then this indicates that the cluster solution is 'good'; there is a good level of cohesion within the clusters and a good level separation between the clusters. Yet, if the score is closer to -1 then this suggests that the cluster solution is 'poor'; there is a poor level of cohesion within the clusters and a poor level of separation between the clusters. Moreover, a cluster solution that is above 0 but lower than .5 is identified as 'fair' (Clemmow, Bouhana & Gill, 2020).

Because this study analyses a range of different online behaviours that could be highly correlated, we ran multicollinearity tests for each of the variables. From the 1089 observations, the highest variance inflation factor (VIF) was <3.4, with the median and mean values being 1.61 and 1.79 respectively. Although there is no firm threshold of acceptable level for VIF, James and colleagues note that 'as a rule of thumb, a VIF value that exceeds 5 or 10 indicates a problematic amount of collinearity' (James et al., 2014; pp.101-102).

Once the typologies of combined online and offline behaviours were identified, this study utilised Max Weber's 'Ideal-types' theory (Weber, 1949) to theoretically construct different terrorist behavioural pathways. As posited by Weber:

> An ideal type is formed by the one-sided accentuation of one or more points of view and by the synthesis of a great many diffuse, more or less present and occasionally absent concrete individual phenomena, which are arranged according to those one-sidedly emphasised viewpoints into a unified analytical construct (Weber cited in Gerhardt, 1994, p.79).

By accentuating that which is deemed important, an ideal-type is not an exact representation of reality but a perspectivist approach to understanding complex social phenomena, which, in this case, is the process of engaging in terrorist activity. Moreover, as suggested by Gerhardt (1994) "perspectivism does not jeopardise the verification and potential validity of an ideal type if the researcher is conscious to the cultural relativity… of his or her approach" (Gerhardt, 1994, p.90), thus, it is important to note that the development of these theoretical constructs are based on what is deemed the purest interpretation of the phenomena and therefore they retain an element of subjectivity.

Nevertheless, the application of Weberian ideal-types provides an analytical framework from which to meaningfully interpret the previously identified clusters of online-offline behaviours. Although its use in terrorism-related research is rare, this approach was recently utilised by Whittaker and Elsayed (2019) who, after conducting a cluster analysis, used ideal-type theory to construct five groups of strategic communication campaigns to be used "as ground for future research… as well as typographically for exposition" (Whittaker and Elsayed 2019; p.20). Furthermore, in the same vein as the aforementioned study, the primary aim of constructing these ideal-types of terrorist pathways was to provide a theoretical framework which can be tested and developed in future research into the online-offline dynamic. To do this, the two authors discussed the results of the cluster analyses together and expanded the results into their purest form, introducing qualitative case studies to help illustrate the types of pathways.

**Results**

*Cluster Analysis*

The first two-step cluster analysis was conducted using the networking behaviours alone and revealed two clusters (Table 1) with a silhouette measure of cohesion and separation of .3, which is considered 'fair' (Clemmow, Bouhana & Gill, 2019). With regard to cluster membership, Network Cluster 1 made up over 70% of the entire sample and the most important predictors of cluster membership were whether actors had maintained contact with a network of co-conspirators online, whether they reinforced their extremist beliefs online and whether they used social media for extremist purposes.

An example of this is Christopher Lee Cornell, a 21 year-old from Ohio who plotted an armed attack on the U.S Capitol Building in 2015 (USA v. Christopher Lee Cornell, 2015). Cornell became known to

authorities by tweeting statements and videos in support of IS and used the platform to express his beliefs to an FBI confidential human source and arrange an offline meeting. On the other hand, in Network Cluster 2, there is Daren Arness Jackson, a 50 year-old from Florida, who provided firearms and firearms training to two individuals, one of whom was an FBI informant, who sought to travel to Syria in 2016 (USA v. Gregory Hubbard, Dayne Antani Christan & Daren Arness Jackon, 2016). According to court documents and media reports, Jackson had no connection to a wider network online and only discussed his beliefs when he met his co-conspirators offline.

| **Networking variables** | **Network Cluster 1 (*n*= 166)** | **Network Cluster 2 (*n*= 65)** |
|---|---|---|
| **Maintained contact with a network online** | 100% | 35% |
| **Reinforced their beliefs online** | 75% | 3% |
| **Social Media for extremist purposes** | 96% | 43% |
| **Shared ideology on an open platform** | 72% | 14% |
| **Disseminated propaganda online** | 49% | 3% |
| **Support others online** | 51% | 5% |
| **Sought legitimisation online** | 40% | 0% |
| **Recruited others online** | 28% | 0% |
| **Used End-to-end encryption** | 26% | 5% |
| **Engaged in an ideological debate online** | 11% | 0% |
| **Maintained contact with a network offline** | 83% | 55% |
| **Recruited others offline** | 21% | 6% |
| **Attended a wider network event** | 7% | 14% |
| **Had a radical family member** | 20% | 29% |
| **Reinforced their beliefs offline** | 43% | 37% |
| **Sought legitimisation offline** | 13% | 9% |

| | | |
|---|---|---|
| **Disseminated propaganda offline** | 10% | 8% |
| **Engaged in an ideological debate offline** | 7% | 8% |

Table (1). Network component clusters

The second two-step cluster analysis was conducted using the event-specific behaviours and likewise discovered two distinct clusters (Table 2). with a silhouette measure of cohesion and separation of .3, which is 'fair' (Clemmow, Bouhana & Gill, 2019). In relation to membership, these clusters were split more evenly than that of the Network clusters, with Event Cluster 2 containing 56% of the actors in the sample and the two most important predictors of event cluster membership were whether the actors had learned and planned for their event offline and whether they had attended a face-to-face meeting with co-ideologues.

Take the case of Said Azzam Mohamad Rahim, a 40-year-old IS recruiter based in Dallas who was arrested for false statements in 2017 (USA v. Said Azzam Mohamad Rahim, 2017). As a member of Event Cluster 1, Rahim never met up with anyone to plan his own travel or an attack, but he did actively encourage others online, using the social media platform Zello and was found to have provided ideological guidence to Salem Abedi, just months before he committed the Manchester Arena attack in 2017.Contrastingly, there is Nicolaus Teausant, who was arrested and charged for attempting to provide material support to IS in 2014 (USA v. Nicolas Teausant, 2014). As a member of Event Cluster 2, Teausant still used the internet to plan but he also met with an undercover operative offline to discuss his intentions to travel to Syria as well as commit an attack within the US.

| **Event variables** | **Event Cluster 1 (*n*= 101)** | **Event Cluster 2 (*n*=130)** |
|---|---|---|
| **Learned and planned offline** | 11% | 98% |
| **Attended an offline meeting to plan their event** | 3% | 87% |
| **Financial co-ordination offline** | 8% | 46% |
| **Trained offline** | 3% | 29% |
| **Learning and planned online** | 69% | 95% |
| **Offline financial transaction** | 33% | 63% |
| **Accessed ideological content online** | 56% | 80% |
| **Prepared for the event online** | 43% | 67% |
| **Experienced a motivating factor online** | 11% | 24% |

| | | |
|---|---|---|
| **Experienced a motivating factor offline** | 17% | 30% |
| **Accessed ideological content offline** | 7% | 17% |
| **Overcame hurdles online** | 3% | 11% |
| **Warned others online** | 4% | 11% |
| **Financial co-ordination online** | 26% | 18% |
| **Warned others offline** | 6% | 7% |
| **Online financial transaction** | 18% | 18% |

Table (2). Event component clusters

Following this, a third and final two-step cluster analysis was conducted using both the network and event clusters to aid the development of typologies that spanned both the networking and event planning components of the terrorist offending process (Table 3). Four typologies made up of different combinations of the network and event component clusters were detected with a silhouette measure of cohesion and separation of .9, which is regarded as 'good' (Clemmow, Bouhana & Gill, 2019). The majority of the actors were represented in the first two typologies. A total of 103 actors (45%) were members of Typology 1, which contained actors who were members of both Network Cluster 1 and Event Cluster 2. Typology 2 contained 63 actors (30%) and consisted of those who were members of Cluster 1 at both the network and the event components. Additionally, 38 actors (16%) were in Typology 3 and categorised those who were in both Network Cluster 2 and Event Cluster 1, meanwhile, the 27 remaining actors (12%) made up Typology 4 and were members cluster 2 at both the network and the event components.

| **Typology (*n*)** | **Network component** | **Event component** |
|---|---|---|
| **Typology 1 *(103)*** | Network Cluster 1 | Event Cluster 1 |
| **Typology 2 *(63)*** | Network Cluster 1 | Event Cluster 1 |
| **Typology 3 (*38)*** | Network Cluster 2 | Event Cluster 1 |
| **Typology 4 (*27)*** | Network Cluster 2 | Event Cluster 2 |

Table 3: Typologies of network and event behaviours

*Terrorist Pathways Ideal-Types*

To draw meaningful inferences about the online-offline dynamic in pathways toward IS terrorist activity, the next stage of the analysis was to theoretically interpret these typologies through the application of Weber's Ideal-types. As discussed above, an ideal-type is formed around the purest interpretation of phenomena and is therefore constructed around the accentuation of its most salient features. With this in mind, the following sub-section describes the characteristics of four ideal-types of terrorist pathways that were identified in the cluster analysis above and further contextualises them through the use of different case studies.

Typology 1: The 'Integrated' Pathway

The actors who were categorised in the 'Integrated' pathway had a proclivity to interact, both online and offline, with a wider network of co-ideologues in both the networking and event planning phases of their terrorist trajectories. While it is somewhat unsurprising that a significant portion of this group executed their plot within a group, it is clear that those who did have an offline network had also maintained virtual contact with individuals beyond their face-to-face conspirators. Take the case of David Wright, who was one of three individuals who had planned an attack on right-wing activist Pamela Geller in 2015 (USA v. David Wright, 2017). Although Wright had interacted both online and offline with his other two co-conspirators, he also maintained an entirely virtual connection to Junaid Hussain, a prominent IS propagandist, and Zulfi Hoxha, an alleged US foreign fighter who later became an influential member of IS. These actors were very much a part of IS' wider radical milieu throughout their networking and attack planning process and utilised the Internet to not only maintain contact with closer peers but network with other like-minded individuals who were not directly involved in their conspiracy.

Typology 2: The 'Encouraged' Pathway

Typically, the actors who were in this pathway were characterised by their heavy use of the Internet throughout both the networking and event planning phases. Although they engaged with a wider network online, they had less contact with co-ideologues offline and therefore utilised the affordances provided by the Internet to plan their eventual terrorist activity. However, while the existence of this pathway does indicate that predominantly online-only trajectories towards terrorist action are plausible, it does not support the notion of 'online-only radicalisation'. On the contrary, it suggests that the dynamics behind terrorist behavioural pathways are deeply complex and can no longer be conceptualised as simply online or offline, but some degree of both. In this regard, those in the "Encouraged" pathway represent actors who have relied more heavily on the online domain throughout their offending process. Consider, for example, the aforementioned case of Zulfi Hoxha, who allegedly travelled to Syria in 2015 (Meleagrou-Hitchens, Hughes and Clifford, 2018). As previously mentioned, Hoxha maintained extensive virtual contact with Wright through social media platforms such as Paltalk and Skype. As well as using this virtual connection to share articles from Dabiq, IS' official magazine, he also received both logistical and financial support from Wright and his co-conspirators.

Typology 3: The 'Isolated' Pathway

The actors in the "Isolated" pathway were defined by their relative lack of co-ideologue interaction across both the online and offline domains. This does not mean there was no interactions at all, but that it was substantially lower than in other pathways. Where the actors within this pathway differed from each other was whether or not they had utilised the Internet to plan their event. Take

Bernard Augustine, a twenty-year-old from California, who is accused of travelling to join IS in Libya (USA v. Bernard Augustine, 2016). Augustine had spent a significant amount of time online, watching IS propaganda videos on YouTube, and conducted several Internet searches about the IS recruitment process. However, he reportedly had no contact with a co-ideologue online or off and took steps to travel to Libya alone. On the other hand, in this same group is Mahad Abdiaziz Abdiraham (State of Minnesota v. Mahad Abdiaziz Abdiraham, 2017). In 2017, Abdiraham had randomly attacked two civilians with a knife at a Mall of America in Minnesota and later claimed he was called upon by the now-deceased leader of IS, Abu-Bakr al Baghdadi. Much like Augustine, Abdiraham had no connections to a network of co-ideologues, yet, while Augustine had utilised the Internet to plan his eventual travel, Abdiraham had seemingly acted at the spur of the moment, with little to no evidence of planning either online or offline.

Typology 4: The 'Enclosed' Pathway

Finally, the 'Enclosed' pathway encompassed the small number of actors who displayed greater network activity offline than they did online, while still utilising the affordances provided by the Internet in the event planning phase of their trajectory. In contrast with those in the "Encouraged" pathway, this typology highlights the possibility of offline-heavy trajectories and provides further support for the complexity behind the online-offline dynamic. Yet, while the individual members of this typology had demonstrated stronger ties to a small group of like-minded peers in their offline environment, it is highly possible that other members of their peer group were immersed within a wider network of co-ideologues, and therefore acted as a mediator between smaller cells and the wider radical milieu. This is certainly the case for several members of the "Minnesota Cluster" (Meleagrou-Hitchens, Hughes & Clifford, 2018, p.39) who had attempted to travel, some of them successfully, to Syria between 2013 and 2017. For example, take the case of Zacharia Yusuf Abdurahman (USA vs. Mohamed Abdirhamid Farah et al., 2015) who attempted to travel to join IS in November 2014. By himself, Abdurahman had no known contact to wider network online, yet he had spent a significant amount of time discussing his support for IS and watching propaganda with a local group of like-minded individuals. This was the same peer-group that Abi Nur (USA vs. Abdullahi Yusuf & Adbi Nur, 2014) had been a part of. Contrary to that of Abdurahman, Nur had been heavily active on Twitter before he had successfully travelled to Syria in 2014 and used the Internet to remain in contact with other members of the Minnesota group even after he had left.

**Discussion and Conclusion**

The results of this study have provided important empirical support for a complex dynamic between the online and offline realms. The sample of IS-inspired terrorist actors displayed high frequencies of network and event-specific behaviours in both domains and several correlations between online and offline equivalents of these behaviours were also identified, illustrating that most actors had split their activities across the two domains. These results largely accord with the findings from prior empirical research into terrorists online and offline behaviours (von Behr et al., 2013; Gill & Corner, 2015; Gill et al., 2017; Gaudete, Scrivens & Venkatesh, 2020; Whittaker 2021). Alongside these pieces of research, this study challenges the conceptually problematic notion that the online domain is simply replacing the offline domain (Sageman, 2008) and provides strong, empirically valid, evidence for terrorist trajectories being cyber-enabled rather than cyber-dependent (Gill et al. 2017).

The most significant contribution that this study has made is via the discovery and development of four ideal-types of terrorist behavioural pathways. In essence, these typologies contrast with the

very notion of ‘online radicalisation’ as implicit in this notion is the idea that the online and offline domains are two separate and autonomous realities; ‘the virtual world’ and ‘the real world’ (Ducol, 2015). As a result, they also contrast with the broader ‘digital dualist’ perspective (Jurgenson, 2012) for, as highlighted in the previous review of the literature, it is this perspective that largely underpins the problematic assertion that ‘radicalisation’ occurs separately in one domain or the other (Omotoyinbo, 2014).

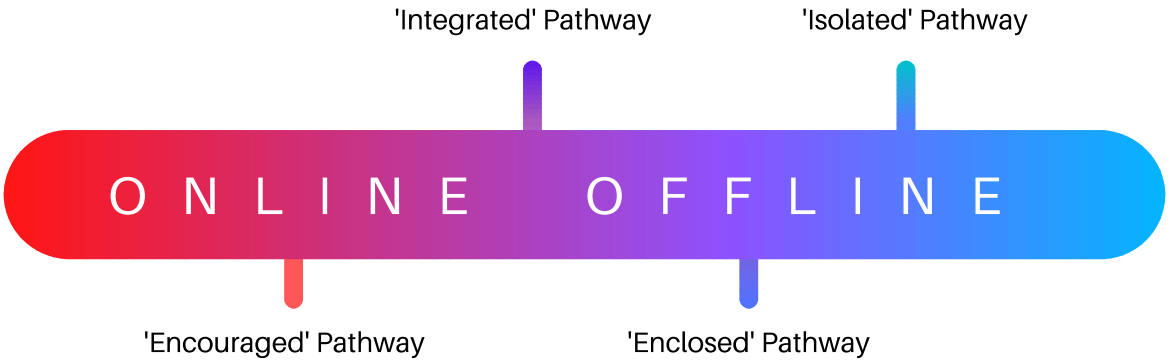


Figure 1: Online/Offline Spectrum

As these typologies collectively illustrate, the reality is significantly more complex. Pathways towards terrorism are not confined to either online or offline but exist on a spectrum in which online and offline are the two most extreme points (Gill et al., 2017). This supports the argument for an ‘augmented reality’ perspective whereby “[one’s] materiality resides not in any one distinct and separate medium” (Rey & Boesal 2014, p.178) but in a complex combination of on and offline. Nevertheless, as the existing literature has been preoccupied with either supporting or challenging ‘online radicalisation’, the discussion has, for the most part, been skewed toward the extreme ends of this spectrum and therefore ultimately fails to acknowledge that there is a significant overlap between the two.

In this regard, these typologies tentatively demonstrate the range of pathways one may take (Figure 1). On one side of the spectrum sit the actors within the ‘Encouraged’ pathway who, as illustrated in the results, had demonstrated higher frequencies of online network and event-specific behaviours. On another side of the spectrum sit the members of the ‘Isolated’ pathway who, for the most part, had displayed minimal pre-event behaviours in either domain. As those in this pathway did not appear to operate in either domain, it might be easy to assume that these actors do not fit on such a

spectrum, yet, it is important to understand that, because the online domain is fundamentally a "digital prosthesis" of the offline environment (Rey & Boesal 2014, p.178), anyone who does not utilise the Internet would, by extension, be more strongly associated with the offline, lived, domain.

Although these two typologies sit closer to the extreme ends of the spectrum, they do not provide support for an online versus offline radicalisation hypothesis. Indeed, this would fail to acknowledge that they exist along a spectrum that is populated with other trajectories toward terrorist activity. As highlighted in the results, almost half of the entire sample of actors were members of the 'Integrated' pathway and therefore demonstrated a mix of online and offline behaviours.

Additionally, through the 'Enclosed' pathway, this study also found a small number of actors who had interacted heavily offline but still utilised the Internet for learning and planning purposes. Such a pathway could be conceptualised toward the offline end of the spectrum, yet it is equally vital to recognise the influence of the online space in their terrorist trajectories. With these different pathways in mind, this study suggests that the extent to which the two domains interact in the process of engaging in terrorist activity will differ based on the specific pathway that an actor is on. Yet, as none of the discovered pathways display trajectories that are entirely in one domain or the other, this study improves upon the understanding of the interaction between the two by adopting a nuanced perspective which concedes that terrorists operate, to at least some degree, in both domains.

*Limitations*

It is also essential to address the study's methodological limitations, particularly in relation to its use of open-source data. As open-source data is largely derived from secondary source information, scholars have criticised their use based on their subjectivity and lack of factual accuracy, both of which can be informed by several biases (Schuurman, 2018). As a result, it is important be cognisant of the context in which a piece of information is written. For example, while criminal complaints can be used to obtain contextually rich data about an individual's behaviours in the lead up to their engagement in terrorist activity, the information was primarily collected for the purpose of an indictment. Similarly, when news sources write about a particular terrorist actor or event, they are largely motivated by generating revenue or increasing their viewership (Whittaker 2019). Yet, it is also important to contextualise why these sources are used so often within the study of terrorism. As suggested by Clemmow and colleagues "the nature of terrorists as a subject of study has required researchers to rely on secondary data collection methodologies to progress" (Clemmow, Bouhana & Gill, 2019, p.22) thus, without this type of data, there would be a fundamental lack of empirical inquiry into the subject of terrorist behaviours.

Another significant issue surrounding the use of open-source information is related to missing and unequal data (Safer-Lichtenstein, LaFree, & Loughran, 2017). As these sources are written for a particular purpose, the authors are likely to capitalise on certain aspects of a case and, as a result, may underreport other key elements. It is, therefore, vital to be aware that when inferences are drawn from these types of sources, they are based on the data that is available. This is a particularly pertinent issue when attempting to examine terrorists online and offline behaviours in equal measure. As scholars, policy makers and the media have emphasised the influence of the Internet in terrorist pathways, the information regarding actors' online activities is richer to that of their offline activities, thus forming the basis of a selection bias whereby online behaviours are emphasised over their offline experiences (Whittaker and Herath 2020).

*Policy and Future Research*

These findings have important implications for both academics and policymakers. The most important proposition is challenging the analytic utility of 'online radicalisation' in contemporary pathways towards terrorism. As an ill-defined and conceptually problematic term, the widespread use of 'online radicalisation' has, as Macdonald and Whittaker (2019) suggest, promoted a sharp division between the online and offline realms and therefore propagated a debate which has focused too heavily on one domain or the other. Moreover, this suggestion is conducive with of that of Gill et al. (2017) who identify concepts such as 'prison radicalisation' (Hamm, 2008, 2013; Sinai, 2014) and 'campus radicalisation' (Thornton, 2011) as similarly problematic and suggest that academics and policymakers are overly focused on the different domains in which 'radicalisation' takes place. Furthermore, rather than using nebulous terminology and focusing on the location where 'radicalisation' takes place, this study proposes that cases be considered in a more holistic manner, attempting to understand risk factors and vulnerabilities. It may be more fruitful to consider the environment in which a would-be terrorist finds themself and how it affects their norm-based motivations (Wikström and Bouhana, 2017; Whittaker 2021). An important aspect of this is to consider why individuals or group (such as our Enclosed or Isolated pathways) may opt *not* to use the Internet given the ease of access, low cost, and almost unlimited source of preparatory information. It is possible that online environments may be so hostile that avoiding the Internet is a rational decision for would-be terrorists (Whittaker 2021; Jensen et al. 2018).

Having demonstrated that different terrorist pathways span online and offline spaces, another important implication for policymakers is to focus on implementing combined online and offline interventions. For the most part, the responses to terrorist use of the Internet have been based online, through disrupting and removing terror-related content, counter- narrative and awareness-based strategic communications campaigns and peer-to-peer messaging via social media (Nasser-Eddine et al., 2011; Berger, 2016; Reed & Ingram, 2019). While recent research has suggested that content removal has been effective in reducing the size of extremist virtual communities in the long-term (Conway et al., 2018), this approach fails to address 'the demand side' of content (von Behr et al., 2013; Edwards & Gibbons, 2013). While online-based strategic communication campaigns focus more on individual supporters, there is a distinct lack of evidence for their effect. One campaign of particular notoriety is the US State Department's, now obsolete, 'Think Again Turn Away' Twitter-based campaign, which focussed "on tweeting counter-messaging material and addressing prominent jihadist accounts" (Katz, 2014, para.2). The initiative attracted many opponents based on its poor execution (Meleagrou-Hitchens, 2017) and it also failed to account for the offline experiences that may lead an individual to seek out such content online. To this end, if one were to only develop online responses to such a complex and multi-level issue, then it is likely that these interventions will fail to have any meaningful effect. Policymakers and practitioners should be cognisant that terrorists act across the two domains and should therefore look to develop interventions that "[create] off-roads for those at risk in the online space which can link into their offline programmes" (Frenett & Dow, 2016, p.24).

This study utilised a sample of entirely IS-inspired actors who were active in the US between 2012 to 2020 to develop a novel method which breaks down the false online-offline dichotomy and explore the different online/offline pathways that terrorists take as part of their trajectories. As a result, the aforementioned findings are culturally and temporally specific. One avenue for future research would be to use the same method to analyse far-right acts of terrorism; the online far right community has been noted as growing and particularly reliant on the Internet (Bowman-Grieve, 2009; Koehler, 2014; Guhl, Ebner & Rau, 2020), but there has still not been a large-scale empirical study to analyse the role of the Internet. It would be instructive to discern whether the same behavioural clusters are predictive in a sample of far-right terrorists or if, for example, they sit

further towards the heavier usage end of the online/offline spectrum compared to jihadist ones. Similarly, scholars have argued that IS terrorists in the US may be more reliant on the Internet than other parts of the world (Soufan Group, 2015; Vidino & Hughes, 2015), making this sample ripe for comparison with IS actors in other parts of the world.

*References*

Alexander, A. (2016) 'Cruel Intentions: Female Jihadists in America', *Program on Extremism*.

Anti-Defamation League (2014) *Homegrown Islamic Extremism in 2013*. New York.

Bacher , J., Wenzig, K., & Vogler, M. (2004). 'SPSS TwoStep cluster - A First Evaluation'. Univ Erlangen-nürnb. https://www.ssoar.info/ssoar/bitstream/handle/document/32715/ssoar-2004-bacher_et_al-SPSS_TwoStep_Cluster_-_a.pdf?sequence=1.

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.

Bastug, M. F., Douai, A. and Akca, D. (2018) 'Exploring the "Demand Side" of Online Radicalization: Evidence from the Canadian Context', *Studies in Conflict & Terrorism*. doi: 10.1080/1057610X.2018.1494409.

Baugut, P. and Neumann, K. (2019) 'Online propaganda use during Islamist radicalization', *Information Communication and Society*, pp. 1–23. doi: 10.1080/1369118X.2019.1594333.

BBC News. (2017). 'Manchester attack: What we know so far', June 12. https://www.bbc.co.uk/news/uk-england-manchester-40008389.

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. doi: 10.1080/1057610X.2016.1141004.

von Behr, I. *et al.* (2013) 'Radicalisation in the Digital Era: The use of the internet in 15 cases of terrorism and extremism', *RAND*. doi: 10.1214/07-EJS057.

Berger, J. M. and 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. (2016). Making CVE Work: A Focused Approach Based on Process Disruption. *ICCT*.

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. doi: 10.1109/ASONAM.2009.31.

Borum, R., 2011c. Rethinking Radicalization. *Journal of Strategic Security*, 4(4), pp.1–6.

Bowman-Grieve, L. (2009). Exploring "Stormfront": A Virtual Community of the Radical Right. *Studies in Conflict and Terrorism*, 32(11), pp. 989-1007.

Castillo, M. *et al.* (2015). 'Paris suicide bomber identified; ISIS claims responsibility for 129 dead,' *CNN*, November 16. https://edition.cnn.com/2015/11/14/world/paris-attacks/index.html.

Chermak, S. *et al.* (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), pp. 191–218. doi: 10.1007/s10940-011-9156-4.

Clemmow, C. *et al.* (2020) 'Disaggregating Lone-actor Grievance-fuelled Violence: Comparing Lone-actor Terrorists and Mass Murderers', *Terrorism and Political Violence*. doi: 10.1080/09546553.2020.1718661.

Clemmow, C., Bouhana, N. and Gill, P. (2020) 'Analyzing Person-exposure Patterns in Lone-actor Terrorism: Implications for threat assessment and intelligence gathering', *Criminology & Public Policy*. doi: 10.1111/1745-9133.12466.

Clifford, B. and Hughes, S. (2018) 'United States vs. Aws Mohammed Younis al-Jayab: A Case Study on Transnational Prosecutions of Jihadi Foreign Fighter Networks', *CTC Sentinel*, (December), pp. 26–30.

Clifford, B. and Powell, H. (2019) 'Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram', *Program on Extremism*, (June).

Conway, M. (2017) 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 40(1), pp. 77–98. doi: 10.1080/1057610X.2016.1157408.

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2018). Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts. *Studies in Conflict and Terrorism*.

Cook, J. and 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*.

Council of the European Union. (2014). 'Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism.' http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf.

Counter Extremism Project. (Nd). Terrorist and Extremist Database. https://www.counterextremism.com/extremists.

Davis, B. R. (2006). 'Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance.' *15 CommLaw Conspectus 119*.

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. New York, NY: Routledge, pp. 82–104.

Edwards, C., & Gribbon, L. (2013). Pathways to Violent Extremism in the Digital Era. *The RUSI Journal*.

European Commission. (2015). 'The European Agenda on Security.' Com. 185. https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf.

EUROPOL. (2016.) 'European Union Terrorism Situation and Trend Report'. https://www.europol.europa.eu/activities-services/main-reports/european-union- terrorism-situation-and-trend-report-te-sat-2016

Everitt, B.S. (1993). *Cluster analysis* (3rd edn.). London: Edward Arnold.

Fisher, A., Prucha, N. and Winterbotham, E. (2019) 'Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability', *Global Research Network on Terrorism and Technology*, (6).

Fitch, K. (2009). 'Making friends in the Wild West: Singaporean public relations practitioners' perceptions of working in social media'. PRism, 6(2).

Frenett, R., & Dow, M. (2016). One to One Online Interventions: A Pilot CVE Methodology. *Institute for Strategic Dialogue*.

Ganor, B. (2002) 'Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?', *Police Practice and Research*, 29(3), pp. 123–133. doi: 10.1080/1561426022000032060.

Gaudette, T., Scrivens, R. and Venkatesh, V. (2020) 'The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists', *Terrorism and Political Violence*. doi: 10.1080/09546553.2020.1784147.

Gerhardt, U. (1994). The Use of Weberian Ideal Type Methodology in Qualitative Data Interpretation: An Outline for Ideal-Type Analysis. *Bulletin de Méthodologie Sociologique*, 45, pp. 74-126

Gill, P. *et al.* (2015) 'What are the Roles of the Internet in Terrorism?', *Vox Pol*. Available at: http://voxpol.eu/wp-content/uploads/2015/11/DCUJ3518_VOX_Lone_Actors_report_02.11.15_WEB.pdf.

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. doi: 10.1111/1745-9133.12249.

Gill, P. (2020) 'The Data Collection Challenge: Experiences Studying Lone-Actor Terrorism', *Resolve Network: Researching Violent Extremism Series*, (February).

Gill, P. and Corner, E. (2015) 'Lone Actor Terrorist Use of the Internet and Behavioural Correlates', in Jarvis, L., Macdonald, S., and Chen, T. M. (eds) *Terrorism Online: Politics Law and Technology*. Abingdon, Oxon: Routledge, pp. 35–53.

Guhl, J., Ebner , J., & Rau, J. (2020). The Online Ecosystem of the German Far-Right. Institute for Strategic Dialogue.

Hecker, M. (2018) '137 Shades of Terrorism: French Jihadists Before the Courts', *Security Studies Center*, (April).

Helfstein, S., 2012. *Edges of Radicalization: Ideas, Individuals and Networks in Violent Extremism*, U.S. Military Academy, Combating Terrorism Center, West Point, NY.

Hamm, M. (2008). Prisoner Radicalization: Assessing the Threat in U.S. Correctional Institutions. NIJ Journal, 261.

Hamm, M. (2013). *The Spectacular Few: Prisoner Radicalization and the Evolving Terrorist Threat*. New York, NY: NYU Press.

HM Government. (2017). 'UK and France Announce Joint Campaign to Tackle Online Radicalisation', June 13. https://www.gov.uk/government/news/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation.

Horan, L., & Beauregard, E. (2017). 'Pathways in the Offending Process of Sex Offenders Who Target Marginalized Victims'. *Journal of Investigative Psychology and Offender Profiling*, 14(4), pp. 213–226.

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.

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. doi: 10.15664/jtr.1159.

Hughes, S., Blackburn, E. and Mines, A. (2019) 'The Other Travelers: American Jihadists Beyond Syria and Iraq', *Program on Extremism*.

Hughes, S. Meleagrou-Hitchens, A., and Clifford, B. (2018). 'A New American Leader Rises in ISIS', *The*

*Atlantic*, January 13. https://www.theatlantic.com/international/archive/2018/01/isis-america-hoxha/550508/.

IBM. (2020). 'Clustering Binary Data'. https://www.ibm.com/support/pages/node/418211

Ingram, H. (2016) 'Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility & Behavioural Change', *International Centre for Counter-Terrorism*, (September 2016). doi: 10.19165/2016.1.12.

Ingram, H. (2018) 'Islamic State's English - language magazines , 2014-2017: Trends & implications for CT-CVE strategic communications', *ICCT Research Papers*. doi: 10.19165/2018.1.15.

Internet World Statistics. (2020). 'World Internet Usage and Population Statistics'. https://www.internetworldstats.com/stats.htm.

James, G., Witten, D., Hastie, T., and Tibshirani, R. (2014). *An Introduction to Statistical Learning: With Applications in R*. New York, NY: Springer Publishing Company.

Jensen, M. *et al.* (2018) 'The Use of Social Media by United States Extremists', *National Consortium for the Study of Terrorism and Responses to Terrorism*.

Jurgenson, N. (2012). 'When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution'. *Future Internet*, 4(1), pp. 83-91.

Katz, R. (2014). 'The State Department's Twitter War With ISIS Is Embarrassing'. *TIME* https://time.com/3387065/isis-twitter-war-state-department/

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. doi: 10.1080/1057610X.2014.974948.

Klausen, J. (2016a) 'A Behavioral Study of the Radicalization Trajectories of American "Homegrown" Al Qaeda-Inspired Terrorist Offenders'.

Klausen, J. (2016b) *The Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990-2015*.

Klausen, J. *et al.* (2016) 'Towards a Behavioral Model of "Homegrown" Radicalization Trajectories', *Studies in Conflict & Terrorism*, 39(1), pp. 67–83. doi: 10.1080/1057610X.2015.1099995.

Klausen, J. *et al.* (2018) 'Radicalization Trajectories: An Evidence-Based Computational Approach to Dynamic Risk Assessment of "Homegrown" Jihadists', *Studies in Conflict & Terrorism*. doi: 10.1080/1057610X.2018.1492819.

Koehler, D. (2014) 'The Radical Online: Individual radicalization processes and the role of the Internet', *Journal for Deradicalization*, (1), pp. 116–134. Available at: http://journals.sfu.ca/jd/index.php/jd/article/view/8%5Cnhttp://journals.sfu.ca/jd/index.php/jd/article/download/8/8.

Krippendorff, K. (2004). '*Content analysis: An introduction to its methodology*'. Thousand Oaks, California: Sage.

LaFree, G. et al. (2018). 'Correlates of Violent Political Extremism in the United States', *Criminology*, 56(2), pp. 233-268.

Levin, B. (2015) 'The Original Web of Hate: Revolution Muslim and American Homegrown Extremists', *American Behavioral Scientist*, 59(12), pp. 1609–1630. doi: 10.1177/0002764215588815.

Macdonald, S. and 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.

Macdonald, S. and Lorenzo-Dus, N. (2019) 'Visual Jihad: Constructing the "Good Muslim" in Online Jihadist Magazines', *Studies in Conflict & Terrorism*, pp. 1–23. doi: 10.1080/1057610X.2018.1559508.

McCauley, C. & Moskalenko, S., 2008. Mechanisms of Political Radicalization: Pathways toward terrorism. *Terrorism and Political Violence*, 20(3), pp.415–433.

Meleagrou-Hitchens, A., Hughes, S. and Clifford, B. (2018) 'The Travelers: American Jihadists in Syria and Iraq', *Program on Extremism, George Washington University*.

Meleagrou-Hitchens, A., Hughes, S. and Clifford, B. (2020) *Homegrown: ISIS in America*. London: I.B. Tauris.

Meleagrou-Hitchens, A. and Kaderbhai, N. (2017) 'Research Perspectives on Online Radicalisation: A Literature Review, 2006-2016', *Vox Pol*.

Moghaddam, F.M., 2005. The Staircase to Terrorism: A Psychological Exploration*. American Psychologist*, 60(2), pp.161–169.

Nanninga, P. (2019) 'Branding a Caliphate in Decline: The Islamic State's Video Output (2015-2018)', *International Centre for Counter-Terrorism*, (April). doi: 10.19165/2019.1.04.

Nasser-Eddine, M., Garnham, B., Agostino, K., & Caluya , G. (2011). Countering Violent Extremism (CVE) Literature Review*. Counter Terrorism and Security Technology Centre*.

Neumann, P., 2013. The Trouble with Radicalization. *International Affairs*, 89(4), pp.873–893.

Norusis, M. (2011). 'Cluster Analysis.' *IBM SPSS Statistics 19 Statistical Procedures Companion*. http://norusis.com/pdf/SPC_v19.pdf

Omotoyinbo, F. R. (2014). 'Online Radicalisation: the Net or the Netizen? *Social Technologies*., 4(1), pp. 51-61

Organization for Security and Co-operation in Europe. (2013). 'Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach.' https://www.osce.org/atu/111438

Pilkington, E., & Roberts, D. (2016). 'FBI and Obama confirm Omar Mateen was radicalized on the internet.' *The Guardian.* June 14. https://www.theguardian.com/us-news/2016/jun/13/pulse-nightclub-attack-shooter-radicalized-internet-orlando.

Post, J., McGinnis, C. and 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. doi: 10.1002/bsl.2123.

Program on Extremism. (Nd). ISIS in America: The Cases. George Washington University. Available at: https://extremism.gwu.edu/cases.

Proulx, J., & Beauregard, E. (2014). 'Pathways in the Offending Process of Extrafamilial Sexual Aggressors Against Women.' In: J. Proulx, E. Beauregard, P. Lussier, & L. Benoit [Eds.] *Pathways to Sexual Aggression*. Abingdon, Oxon: Routledge, pp. 71-110.

Ramsay, G. (2015) 'Why terrorism can, but should not be defined', *Critical Studies on Terrorism*, 8(2),

pp. 211–228. doi: 10.1080/17539153.2014.988452.

Reed, A., & Ingram, H. (2019). A practical guide to the first rule of CT- CVE messaging: Do Violent extremists no favours. *Europol.*

Rey, P. J., & Boesel, W. E. (2014). 'The Web, Digital Prostheses, and Augmented Subjectivity. In: Kleinman, D.L. & Moore, K., [Eds.] *Routledge Handbook of Science, Technology, and Society*. Abingdon, Oxon: Routledge, pp. 173-188.

Reynolds, S. C. and Hafez, M. M. (2017) 'Social Network Analysis of German Foreign Fighters in Syria and Iraq', *Terrorism and Political Violence*, (April). doi: 10.1080/09546553.2016.1272456.

Safer-Lichtenstein, A., LaFree, G. and 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. doi: 10.1177/1043986217697873.

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. doi: 10.2307/25462270.

Schmid, A. P. (2004) 'Terrorism - The definitional problem', *Case Western Reserve Journal of International Law*, 36(2), pp. 375–419.

Schuurman, B. (2018) 'Research on Terrorism, 2007–2016: A Review of Data, Methods, and Authorship', *Terrorism and Political Violence*, pp. 1–16. doi: 10.1080/09546553.2018.1439023.

Schuurman, B. & Taylor, M., 2018. Reconsidering Radicalization: Fanaticism and the Link Between Ideas and Violence. *Perspectives on Terrorism*, 12(1), pp.3–22.

Sedgwick, M., 2010. The Concept of Radicalization as a Source of Confusion. *Terrorism and Political Violence*, 22(4), pp.479–494.

Silber, M.D. & Bhatt, A., 2007. Radicalization in the West: The homegrown threat. *New York City Police Department*.

Sinai, J. (2014). Developing a model of Prison Radicalisation. In A. Silke [Ed.], *Prisons, Terrorism and Extremism: Critical Issues in Management, Radicalisation and Reform*. New York, NY: Routledge. pp. 35-46.

Skinner, C. (2015) 'Punishing Crimes of Terror in Article III Courts', *Yale Law & Policy Review*, 31(2).

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.

START. (Nd). Global Terrorism Database. Available at: https://www.start.umd.edu/gtd/

START (2018) 'Profiles of Individual Radicalization in the United States (PIRUS) Codebook'. Available at: www.start.umd.edu.

Stebbins, R. (2001). *Exploratory Research in the Social Sciences*, Thousand Oaks, CA: Sage Publications.

Stefanska, E. *et al.* (2015). 'Offense Pathways of Non-Serial Sexual Killers.' *Journal of Criminal Justice*,

43(2), pp. 99-107.

Stohl, M. (2008) 'Old Myths, New fantasies and the Enduring Realities of Terrorism', *Critical Studies on Terrorism*, 1(1), pp. 5–16. doi: 10.1080/17539150701846443.

Thornton, R. (2011). Counterterrorism and the neo-liberal university: providing a check and balance? *Critical Studies on Terrorism,* 4(3), pp. 421-429.

Tsukayama, H. *et al*. (2016). 'Gunman who killed 49 in Orlando nightclub had pledged allegiance to ISIS' *The Washington Post*, June 13. https://www.washingtonpost.com/news/post-nation/wp/2016/06/12/orlando-nightclub-shooting-about-20-dead-in-domestic-terror-incident-at-gay-club/.

UN CTED (2015) *Analysis and recommendations with regard to the global threat from foreign fighters*.

Vidino, L. & Hughes, S., 2015. ISIS in America: From Retweets to Raqqa, *George Washington University Program on Extremism*.

Weber, M. (1949). 'Objectivity' in Social Science and Social Policy'. In H. Finch, & E. Schils [Eds.], *The Methodology of the Social Sciences*. New York, NY: New York Free Press.

Weimann, G. (2012) 'Lone Wolves in Cyberspace', *Journal of Terrorism Research*, 3(2), pp. 75–90.

Whittaker, J. (2019) 'Building Secondary Source Databases on Violent Extremism: Reflections and Suggestions', *Resolve Network: Researching Violent Extremism Series*, (July).

Whittaker, J., & Herath, C. 'Understanding the Online and Offline Dynamics of Terrorist Pathways,' *Global Network on Extremism & Technology.* https://gnet-research.org/2020/07/13/understanding-the-online-and-offline-dynamics-of-terrorist-pathways/.

Whittaker, J. (2021) 'The Online Behaviors of Islamic State Terrorists in the United States', *Criminology & Public Policy*. doi: 10.1111/1745-9133.12537.

Whittaker, J. and Elsayed, L. (2019) 'Linkages as a Lens: An Exploration of Strategic Communications in P/CVE', *Journal for Deradicalization*, 20, pp. 1–46.

Wikström, P. O. H. and Bouhana, N. (2017) 'Analyzing Radicalization and Terrorism: A Situational Action Theory', in LaFree, G. and Freilich, J. D. (eds) *The Handbook of the Criminology of Terrorism*. Chichester: John Wiley & Sons, pp. 175–186. doi: 10.1002/9781118923986.ch11.

Winter, C. (2015) 'Detailed Analysis of Islamic State Propaganda Video: Although the Disbelievers Dislike It', *Quilliam Foundation*.

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.

*Cases Cited*

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

USA v. Bernard Augustine, Criminal Complaint, Case 1:16-mj-01107-MDG, United States District Court for the Eastern District of New York, 2016.

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

USA v. Houcine Bechir Ghoul, Criminal Complaint, Case 5:17-mj-1683-JG, United States District Court for the Eastern District of North Carolina.

USA v. Gregory Hubbard, Dayne Antani Christian, and Darren Arness Jackson, Criminal Complaint, Case 9:16-cr-80107, United States District Court for the Southern District of Florida, 2016.

USA v. Said Azzam Mohamad Rahim, Criminal Complaint, Case 3:17-mj-00171-BK, United States District Court for the Northern District of Texas, 2017.

USA v. Akhror Saidakhmetov, Defendant's Sentencing Memorandum, Case 1:15-cr-00095-WFK, United States District Courts for the Eastern District of New York, 2017.

USA v. Nicholas Teausant, Criminal Complaint, Case 2:14-mj-0064, United States District Court for the Eastern District of California, 2014.

USA v. David Wright, Government's Sentencing Memorandum, Case 1:15-cr-10153-WGY, United States District Court for the District of Massachusetts, 2017.

USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint, Case: 14-MJ-0124, United States District Court for the District of Minnesota, 2014.