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

Whittaker, J.J.

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."

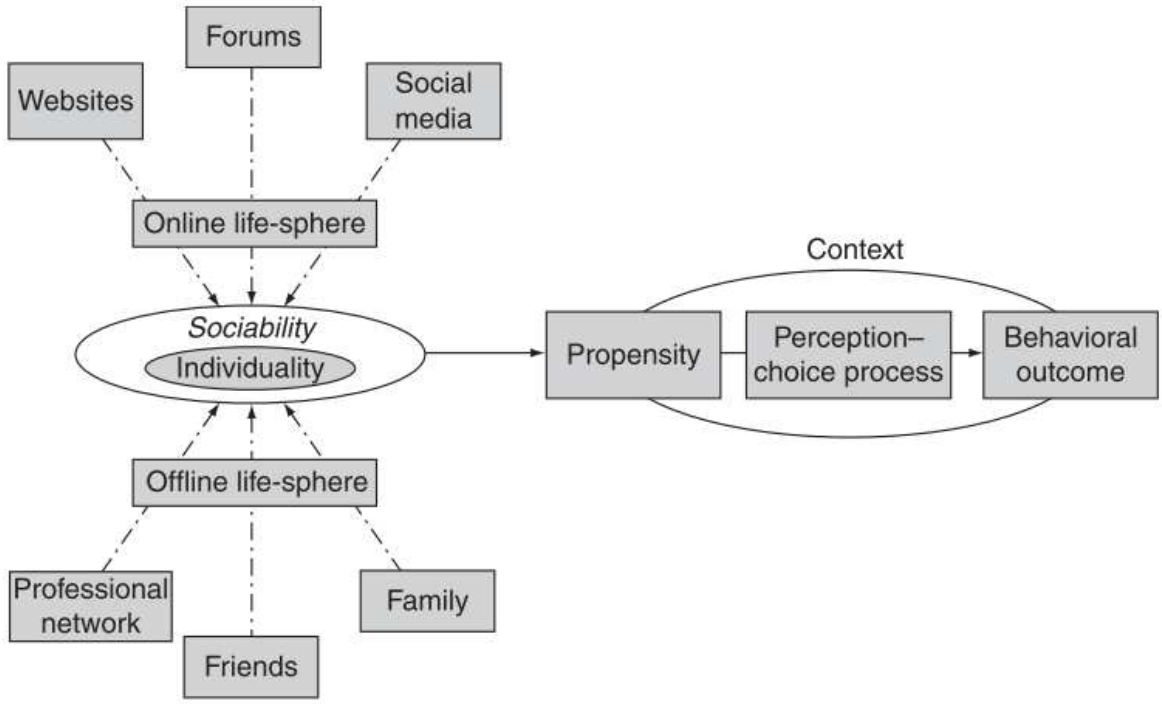


Figure 20 - Ducol's (2016) "Life Spheres" SAT Framework

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.

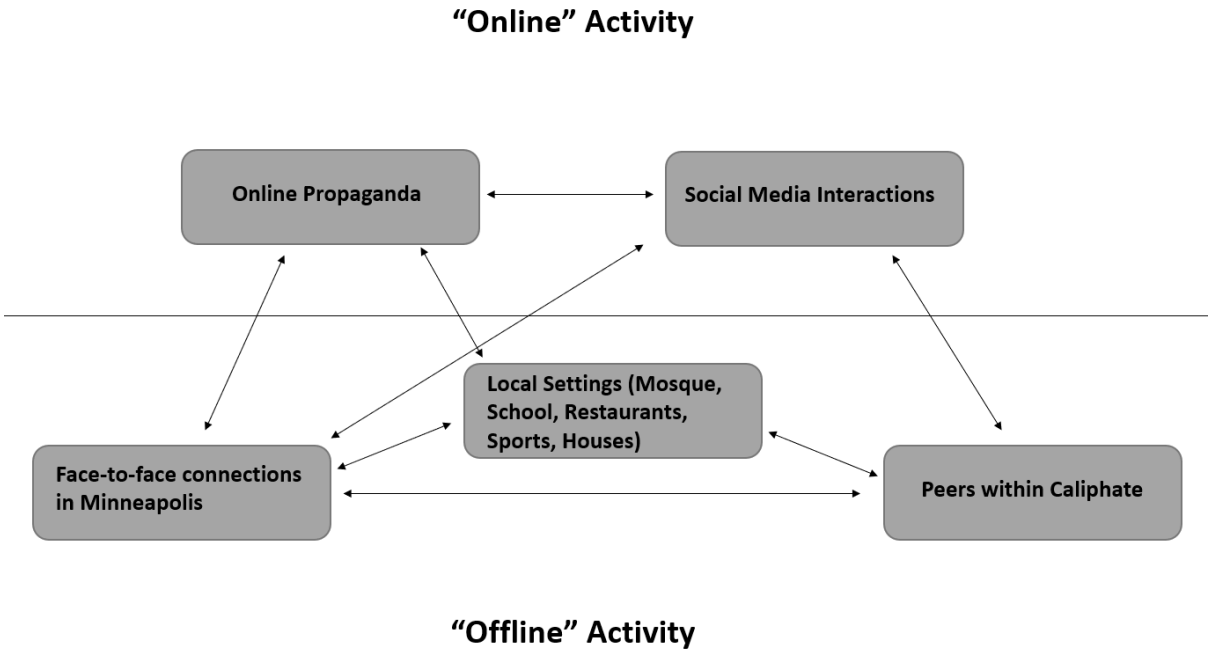


Figure 21 - Yusuf's Online vs Offline Activities

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.

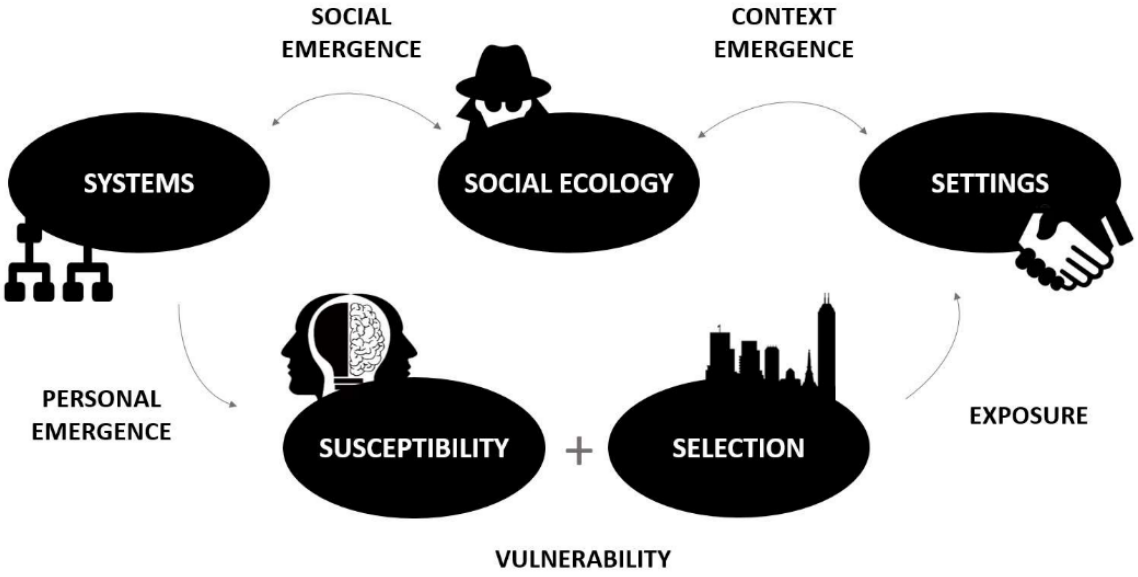


Figure 22 - Bouhana's (2019) S5 Inference Framework

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

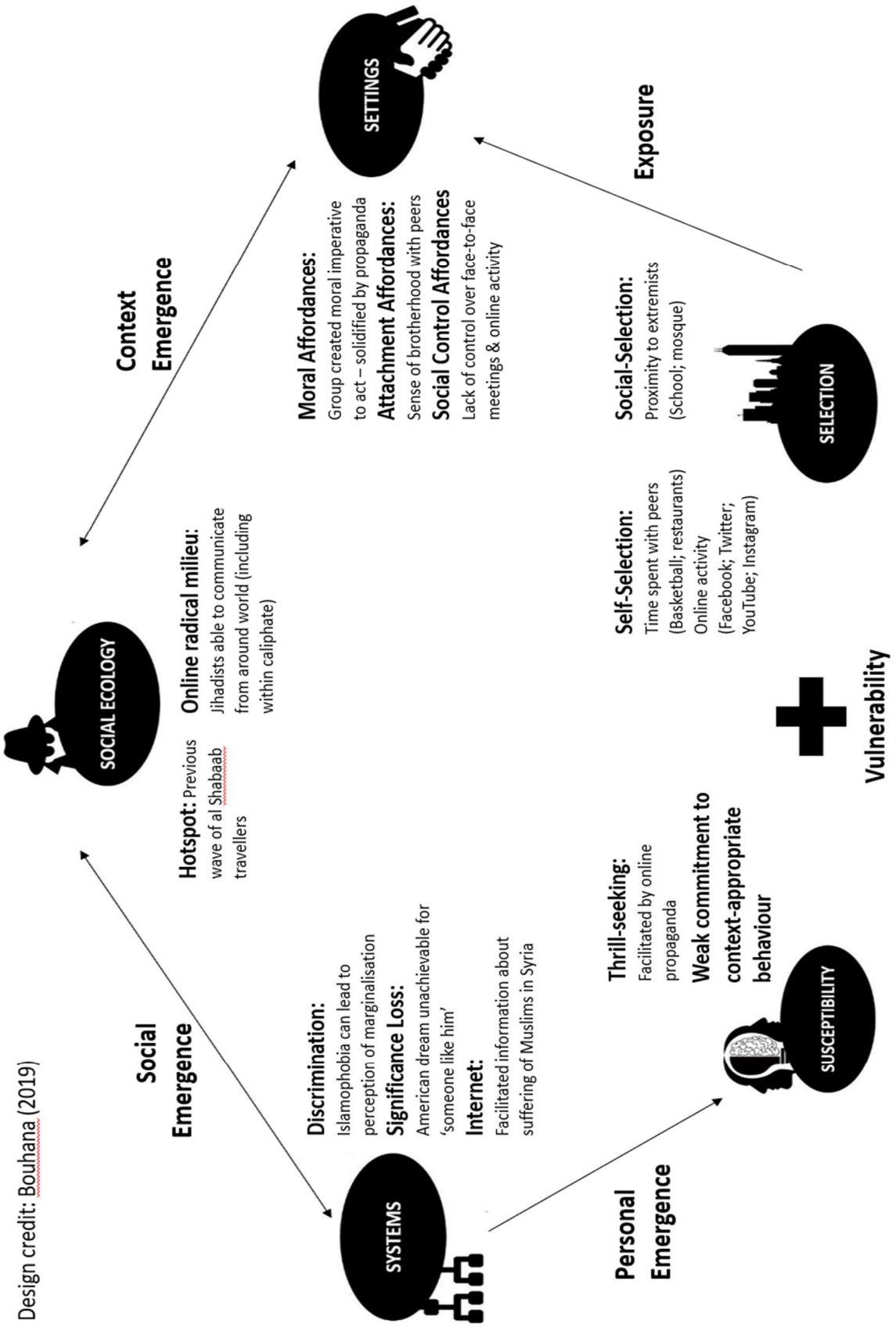
[359] Temple-Raston. He Wanted Jihad. He Got Foucault.
[360] USA v. Abdirizak Warsame, Criminal Complaint.
[361] Koerner, Can You Turn a Terrorist Back into a Citizen?
[362] Temple-Raston. He Wanted Jihad. He Got Foucault.
[363] Koerner, Can You Turn a Terrorist Back into a Citizen?
[364] Temple-Raston. 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.