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

Whittaker, J.J.

Chapter 8: Conclusion

This project began with a desire to better understand the phenomenon of "online radicalisation" in the era of social media. It was prescient because, in recent years, the world has seen the rise of one of the biggest and most dangerous terrorist organisations – IS – who conducted numerous attacks and to whom tens of thousands of individuals travelled to join. The group is particularly noteworthy because their online communication strategy was repeatedly described as sophisticated and wide-reaching, leading to the inevitable suggestion that individuals had radicalised online when they joined the group or acted on its behalf.

8.1 Summary and Key Findings

While this thesis is empirical in nature, each chapter is required as a separate step in successfully conceptualising and analysing the phenomenon under study. Chapter 2 highlights the conceptual ambiguity surrounding the word "radicalisation" – different scholars use it interchangeably to denote the process of becoming a terrorist, extremist, and radical. The key difference is whether it denotes a behavioural or cognitive process. These problems spill over into the conceptualisation of "online radicalisation" too and add to extra ambiguities surrounding what constitutes being sufficiently "online." There have been many attempts to theorise and model the process of radicalisation, although they tend to remain in the theoretical realm and have not been subjected to rigorous testing. Despite this, there is a growing literature which empirically analyses radicalisation; although there is no common pathway or terrorist profile, certain demographic, socioeconomic, personality, and experiential factors may appear more frequently than one would expect in the general population.

Chapter 3 surveys the existing literature on online radicalisation. As with the literature on radicalisation more generally, several scholars have attempted to theorise or model the process. These theoretical contributions have not yet adequately explained how the Internet affects radicalisation; most assume (or explicitly state) problematic assumptions, such as a relationship between engaging with radical content and becoming a terrorist or an ontological distinction between the online and offline domains. Empirical research into the "demand" side of online radicalisation tends to demonstrate that if one understands the process as the Internet replacing offline interactions in pathways towards terrorism, then it has not become the new norm. Rather, online and offline dynamics tend to complement each other. However, other findings suggest that the Internet may provide an important space for the construction of a radical identity, which may be fundamentally different online than off. An analysis of the literature on the "supply" side of terrorist content shows that up until around 2016, IS ran one of the most sophisticated and wide-reaching propaganda campaigns – primarily online – of any terrorist or extremist group in history. This highlights the importance of undertaking

data-driven research on IS actors to establish whether they are more reliant on the Internet than previous cohorts of terrorists, and if so, in what ways.

Chapter 3 concludes by establishing four research questions derived from the academic literature which are used for the quantitative analysis in the thesis: i) How frequently do terrorists use the Internet, and in what ways? ii) Has the online domain replaced the offline as the primary venue for radicalisation? iii) Do terrorists that act online demonstrate different experiences to those that do not? iv) Does acting on the Internet help or hinder terrorists?

Chapters 2 and 3 show that there are several conceptual problems underlying the study of contemporary pathways towards terrorism and the role of the Internet. Chapter 4 lays out the methodological groundwork for studying the phenomenon robustly and empirically. Rather than a focus on an ill-defined, abstract concept, it focuses specifically on discrete and observable behaviours collected from open sources. The chapter outlines the research design, methods of data collection, inclusion and exclusion criteria, the coding system, the methods of analysis, as well as ethical considerations.

Chapter 5 undertakes a quantitative analysis using a codebook developed from the academic literature to answer the four research questions outlined above. Before this, a demographic snapshot of the sample is presented which suggests that terrorist actors come from a range of backgrounds and life paths. However, as with the existing literature, commonalities appear; the sample is predominantly male, young and errs on the lower end of the socioeconomic spectrum. Converts appear to be over-represented, as do those with a criminal record. The findings of RQ1 suggest that the Internet is ubiquitous in contemporary terrorist pathways; actors used the Internet for a wide range of antecedent behaviours across several online platforms. Comparison with similarly coded studies suggests that terrorists may be using the Internet more than in previous years. Building on this, RQ2 finds that there is little reason to believe that online radicalisation is replacing offline; terrorists that engaged in a range of antecedent behaviours were significantly more likely to also act offline too.

Although the findings of RQ3 were more mixed, they generally pointed towards a similar experience for individuals that use the Internet and those that do not. For example, lone actors were *not* more likely to use the Internet than group-based ones, neither were individuals that plotted more sophisticated attacks. Finally, RQ4 shows that using the Internet may actually be hampering would-be terrorists' plots – individuals that acted online were less likely to be successful than those that did not. Taking all four RQs together, this chapter demonstrates the complexity of the relationship between terrorism and the Internet. One may be inclined to observe that most terrorists use the Internet as part of their plots and take that to mean they are radicalising online. However, Chapter 5 underscores the importance of offline interactions and the interrelated nature of the two domains.

The quantitative analysis of Chapter 5 provides an important overview of the sample as a whole. Chapter 6 supplements this with an inductive analysis of the sample's online behaviours using a methodology inspired by Grounded Theory. While Chapter 5 is limited to a codebook which mostly consisted of binary yes/no answers, this chapter explores emergent themes which are grounded in the data and derives three radicalisation dynamics. Firstly, rather than being seen as a direct motivator to act, terrorists' consumption of propaganda can also be seen as an ongoing socialisation process in which actors engage with the radical milieu to network, discuss, and construct radical identities. Secondly, for radicalising females, the Internet may offer a space for them to perform a less restricted gender identity than offline Salafi jihadist networks would allow. Finally, the vast information abundance of the Internet offer would-be terrorists a "buyers' market" to fulfil their needs in a flexible and constraint-free way. Taking these findings together, Chapter 6 reinforces the notion that radicalisation is invariably a social process; concepts such as self-radicalisation are largely redundant because even when acting online, terrorists are attempting to communicate, befriend, and network with others. The chapter also demonstrates the malleability of the online space – individuals are free to act with fewer limitations and build identities which reflect this freedom.

Finally, Chapter 7 synthesises the thesis into its original contributions. This thesis makes an important empirical contribution by adding to a nascent literature of data-driven studies which analyse the role of the Internet in contemporary radicalisation. Moreover, it draws from a complementary mixed method approach which goes beyond simply looking at online behaviours, instead considering them in relation to offline factors. There are also theoretical contributions at three levels of abstraction – the radicalisation dynamics established in Chapter 6; an ontological challenge based on the false dichotomy of attempting to separate online from offline activities; as well as demonstrating why a more holistic view of radicalisation – Bouhana's (2019) 5S framework – is a better tool for understanding the use of the Internet than existing online radicalisation theories. Chapter 7 then discusses the main policy contribution of this thesis, that the radical jihadist ecosystem is fragile and existing policy solutions may have unintended consequences that are harmful in the long run. After highlighting these contributions, it turns to the limitations of the study, which include focusing specifically on a single group and country; a lack of measurable base-rates for comparisons; the use of secondary sources; and the subjective nature of coding. Chapter 7 finishes by discussing avenues for future research, including testing the hypotheses which are generated in Chapter 6, analysing terrorist pathways via sequential analysis, researching social media affordances, as well as looking to the future to establish if new trends emerge.

8.2 Informing Policymakers and the Media

Despite this thesis and previous research pointing towards online radicalisation as a complex process, there is a need for these findings to inform decision makers and those with platforms that can effectively communicate these contributions to the public. As discussed above, popular media outlets often ascribe the Internet with radicalising

agency, as if there is something inherent which can dramatically alter an individual's trajectory. As both the empirical findings of this research and the review of the literature in Chapter 3 demonstrate, there is little reason to believe this is the case. Filter bubbles and online echo chambers do exist, but we do not know enough to say if they exacerbate individuals' pathways; terrorist propaganda is plentiful but the evidence-base for experimentally testing whether it is effective is still in its infancy. On the other hand, this research and others' has repeatedly highlighted that online interactions may be overrated in importance. However, the message that is often relayed to the public, via the media, is one that is confident that the Internet poses a substantial threat. Headlines such as "YouTube, the Great Radicalizer" (Tufekci 2018) or "Beware the Rabbit Hole of Radicalization" (Washington Post Editorial Board 2019) in the *New York Times* and *Washington Post* respectively are relatively typical of a narrative which not only places the Internet as the primary venue for this process, but often suggest that it has been some kind of "game changer" for terrorism.

This line of thinking is seemingly mirrored by policymakers, particularly in the United Kingdom, whose government recently published their *Online Harms White Paper*, which warns against 'terrorists, including Islamist groups such as [IS] and [AQ] as well as far right terrorists, [who] use the internet to spread propaganda designed to radicalise vulnerable people' (HM Government 2019, p.11). The white paper suggests that platforms that do not do enough to prevent this type of content could be faced with fines, ISP blocking, and criminal liability for executives. Similarly, in 2019, the UK Parliament passed a bill which increased the maximum sentences for terrorism precusor offences such as the dissemination of propaganda from seven to fifteen years (Counter-Terrorism and Border Security Act 2019). In February 2020, the Home Secretary said she was looking to "toughen up" these laws by creating a new offence of possessing terrorist material (Siddique and Grierson 2020). To be clear, there is a debate to be had over the virtues and pitfalls of removing terrorist content from the Internet that goes beyond the scope of this research. However there is little reason to believe that, as the *Online Harms White Paper* implies, that it will reduce terrorism. Rather, this research suggests that terrorists' ability to operate on the Internet may help law enforcement's investigations against terrorists. Moving forward, it is important for researchers to communicate nuanced findings to interested parties such as the media and policymakers so they do not create detrimental unintended consequenses or end up giving undue focus to one specific aspect of a much larger picture.

8.3 Towards an Evidence-based Understanding of Terrorist Pathways

Scholars have long lamented the dearth of empirical data which analyses the role of the Internet in pathways towards terrorism (Gill et al. 2017; von Behr et al. 2013). Rather than study the individual trajectories of terrorists – i.e. the demand-side – research into terrorists' use of the Internet has largely focused on the supply of content available to terrorists online. While this research is valuable and has informed this project, an over-reliance on the supply of content leaves a gap in the body of literature. This gap is

understandable, it is far easier for researchers to study online content – which terrorist groups often go to great lengths to make publicly available – than to wrestle with the practical and ethical issues of researching individual terrorists' experiences. However, analyses of the supply of content often suggest a degree of causality of influence over the individual that engages with it, which cannot be proven (von Behr et al. 2013).

This research has added to the small body of literature which bridges this gap, providing quantitative and qualitative analyses which simultaneously draw from previous research while using inductive methods of enquiry. This thesis demonstrates that it is possible to research this topic robustly without access to primary data; it remains difficult to conduct interview-based research with terrorists or to look at their private online records. However, there is a wealth of rich and granular data available from open sources. Ironically, the perception of the Internet as the primary venue for pathways towards terrorism increases the likelihood that online interactions will be mentioned in court documents or news sources, which has aided this research greatly. I hope that scholars of future research draw upon these methods of data collection to study the phenomenon further and that governments understand the value in making such sources available, either by making them accessible for anybody or sharing closed-source data such as police records with trusted researchers.