Onlife Radicalisation: Understanding the Online/Offline Nexus

CONFERENCE PUBLICATION

DATE

14-15/03/2023

AUTHORS

Joe Whittaker

This paper was presented at the 4th conference of the European Counter Terrorism Centre (ECTC) Advisory Network on terrorism and propaganda, 14-15 March 2023, at Europol Headquarters, The Hague. The views expressed are the authors' own and do not necessarily represent those of Europol.

1. Introduction

The concept of online radicalisation has become ubiquitous in discussions around terrorism. Policymakers regularly highlight it as a key threat. French President Emmanuel Macron and former UK Prime Minister Theresa May established a joint UK-French initiative to tackle online radicalisation, including stronger regulations against tech companies that fail to remove terrorist content, which was endorsed by the Dutch Prime Minister Mark Rutte[1]. The EU Council also highlighted the danger of online radicalisation, vowing to counter it using several methods including disruption of terrorists' use of the Internet and by challenging groups' ideologies[2]. It is a concern for law enforcement too; the most recent Europol Terrorism Situation and Trend Report points to the threat from right-wing lone actor terrorists who have radicalised online as being one of the most significant threats[3], while the FBI emphasise the danger too, suggesting that terrorists often radicalise online and mobilise to violence quickly[4]. However, in recent years, there have been critiques of the concept and suggestions that it is not fit for purpose.

This paper seeks to expand upon these critiques by arguing that the concept is fundamentally flawed. It will do this in three ways: Firstly, by discussing the ways in which online radicalisation does not stand up to empirical scrutiny. Secondly, by demonstrating that in the contemporary world of communications technology, it is impossible to separate acting 'online' from 'offline', but rather the two domains are inseparably intertwined. We inhabit a new domain which is often referred to as 'onlife'. Finally, rather than focusing on whether an individual radicalised online or offline, we should instead opt for more holistic theories of radicalisation which take an individual's full information environment into account. To do this, the paper will draw on a case study of a would-be Islamic State (IS) foreign fighter – Abdullahi Yusuf – and Bouhana's 5S Framework of radicalisation to show the complexity of the interplay of communication technologies within different factors in radicalisation, which in turn, show why attempting to demarcate between 'online' and 'offline' radicalisation is a fruitless endeavour.

2. Online radicalisation

Over the past two decades, researchers have attempted to understand and explain how the Internet can affect radicalisation. Even before the notion of 'online radicalisation' became popular in the late 2000s[5], scholars argued that there were fundamental differences between the online and offline domains that may exacerbate individuals who are already at risk of political violence. These include: perceived

[1] HM Government (2017). "UK and France Announce Joint Campaign to Tackle Online Radicalisation", gov.uk/government/news/uk-and- france-announce-joint-campaign-to-tackle-online-radicalisation.
[2] Council of the European Union (2014). "Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism", data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf.
[3] Europol (2023). "Terrorism Situation and Trend Report", europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat.
[4] Federal Bureau of Investigation (nd). "What We Investigate – Terrorism", fbi.gov/investigate/terrorism.
[5] Whittaker, J. (2022). "Online Radicalisation: What We Know", Radicalisation Awareness Network Policy Support – European Commission.

anonymity; online disinhibition effects; non-hierarchical structures; the effects of online propaganda; the formation of echo chambers; deindividuation; as well as 'role playing' an idealised version of themselves for a perceived audience[6]. As the Internet became ubiquitous in day-to-day life, cases of radicalisation simultaneously seem to become more reliant on the Internet, leading to eminent terrorism scholar Marc Sageman declaring that "face-to-face radicalisation has been replaced by online radicalisation"[7]. Despite the widespread concern, the research into the theory of online radicalisation has been criticised for not being derived from empirical data, but rather 'borrowed' from potentially analogous social science research as well as drawing heavily from anecdotal evidence[8]. The research also tends to place the consumption of propaganda as a key element of the process, although this is a complex phenomenon and when tested often demonstrates equivocal empirical results[9]. Noteworthy for the purposes of this research, the basis of this literature argues that the online domain is a distinct and separable space from the offline one. This will be challenged below, placing the entire notion of 'online radicalisation' in jeopardy.

Although terror plots have an ever-increasing cyber footprint, empirical research has repeatedly demonstrated that terrorists tend to act in both domains. Analysing the radicalisation pathways of 223 convicted terrorists in the UK, Gill and colleagues observe that "there is no easy offline versus online violent radicalization dichotomy to be drawn…Plotters regularly engage in activities in both domains"[10]. Similarly, in research on 231 individuals that acted on behalf of IS in the US, Whittaker also finds that behaviours were spread over both domains. He argues that the "melding of the online and offline environment lends further credence to the argument that it is a false dichotomy"[11]. Expanding on this dataset, Herath and Whittaker conduct a cluster analysis to create four typographical radicalisation pathways. They find that each of the pathways exists on a spectrum of online and offline behaviour, suggesting that the notions of 'online' or 'offline' radicalisation are simplistic[12]. Hamid and Ariza find that the majority of their sample of 439 terrorists were radicalised 'mostly offline' while only around 2% could be classified as 'online asocial radicalisation' and 18% as 'mostly online'[13]. Similarly, conducting closed-source data with prisoners in the UK, Kenyon and colleagues find that although the use of the Internet was increasing, it was not replacing offline interactions – rather individuals tended to operate in both domains[14].

[6] For example, see: Neumann, P. (2013). "Options and Strategies for Countering Online Radicalization in the United States", *Studies in Conflict & Terrorism*, Vol. 36, Issue 6, pp. 431–459; Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. University of Pennsylvania Press, Philadelphia, PA.; Suler, J. (2004). "The Online Disinhibition effect", *CyberPsychology & Behavior*, Vol. 7, Issue 3, pp. 321–326; Brachman, J. M. and A. N. Levine (2011). "You Too Can Be Awlaki", *The Fletcher Forum of World Affairs*, Vol. 35, Issue 1, pp. 25–46.

[7] Sageman, M. (2008). "The Next Generation of Terror", *Foreign Policy*, (March/April), pp. 36–42.

[8] Whittaker, J. (2022). "Rethinking Online Radicalisation", *Perspectives on Terrorism*, Vol. 16, Issue 4, pp. 27-40.

[9] For example, see: Braddock, K., Schumann, S., Corner, E. and Gill, P. (2022). "The Moderating Effects of 'Dark' Personality Traits and Message Vividness on the Persuasiveness of Terrorist Narrative Propaganda", *Frontiers in Psychology*, 13; Braddock, K., Hughes, B., Goldberg, B. and Miller-Idris, C. (2022). "Engagement in Subversive Online Activity Predicts Susceptibility to Persuasion by Far-right Extremist Propaganda", *New Media & Society*.

[10] Gill, P. et al. (2017). "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes", *Criminology and Public Policy*, Vol. 16, Issue 1, p. 114.

[11] Whittaker, J. (2021). "The Online Behaviors of Islamic State Terrorists in the United States", *Criminology and Public Policy*, Issue 20, p. 195.

[12] Herath, C. and J. Whittaker (2021). "Online Radicalisation: Moving Beyond a Simple Dichotomy", *Terrorism and Political Violence*, Vol. 35, Issue 5, pp.1027-1048.

[13] Hamid, N. and C. Ariza (2022). "Offline Versus Online Radicalisation: Which is the Bigger Threat?", *Global Network on Extremism & Technology*.

[14] Kenyon, J., Bender J. and C. Baker-Beall (2022). "Understanding the Role of the Internet in the Process of Radicalisation: An Analysis of Convicted Extremists in England and Wales", *Studies in Conflict and Terrorism*.

However, it should be noted that updated research looking at individuals convicted from 2018-2021 demonstrates an increasingly prominent role for the Internet[15].

3. Onlife radicalisation

So far, this paper has discussed research which seeks to understand the differences between online and offline terrorist activity. However, there is reason to doubt whether this is an analytically useful distinction. For over a decade, Internet philosophers have been calling this into question, suggesting that the two domains are now inseparably linked, and it no longer makes sense to dichotomise between the two domains; this new reality has been termed 'Onlife'[16]. Both domains now enmesh in a combined reality in which the Internet – and in particular social media and mobile data – supplements our offline lives. Nothing on the Internet exists outside of longstanding social constructions, but these are now implanted into a new augmented reality[17]. Humans no longer 'go online,' but instead are connected 24/7 (devices still collect data on subjects when they are asleep, which affects their online experience). This 'augmented subjectivity' is a single unified reality which is co-produced in both domains and can no longer be isolated, but instead is inextricably enmeshed[18]. This reality has led to some important transformations: a blur between reality and virtuality; an unclear distinction between human, machine and nature; a reversal between information scarcity and abundance; and a shift from the primacy of stand-alone things, properties and binary relations to the primacy of interactions, processes and networks[19].

If attempting to separate the online and offline domain is an impossible task, then it puts the notion of 'online radicalisation' in jeopardy. Valentini, Lorusso and Stephan contend that contemporary radicalisation takes place in onlife spaces in which the two domains conflate in unprecedented ways: "radicalization processes evolve, and develop, by integrating elements that pertain to both"[20]. They articulate this point by discussing the role of social media recommendation systems, which have been shown in some circumstances to amplify extremist content towards users and potentially cause a 'filter bubble' effect[21]. Although algorithmic amplification may seem like an online experience, Valentini and colleagues note that recommendation systems draw heavily on both domains such as browsing history, physical location and demographic factors[22]. Whittaker argues that the notion of online radicalisation is redundant and we must re-ontologise the concept. He draws on examples of terrorists' engagement with propaganda, which is often framed as a key part of online radicalisation, noting that this behaviour crosses through both domains; individuals would watch online propaganda with their face-to-face networks, discussing it together afterwards and

[15] Kenyon, J., Bender J. and Baker-Beall, C. (2022). *The Internet and radicalisation pathways: Technological advances, relevance of mental health and role of attackers*, Ministry of Justice Analytical Series.

[16] Floridi, L. (2015). "Introduction" in Floridi, L. (Ed.) *The Onlife Manifesto: Being Human in a Hyperconnected Era*, SpringerOpen, London , pp. 1–7.

[17] Jurgenson, N. (2012). "When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution", *Future Internet*, Vol. 4, Issue 1, pp. 83–91.

[18] Rey, P. J. and W. E. Boesel (2014). "The Web, Digital Prostheses, and Augmented Subjectivity", *Routledge Handbook of Science, Technology, and Society*, January 2014, pp. 173–188.

[19] Floridi, L. et al. (2015). "The Onlife Manifesto" in Floridi, L. (Ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, SpringerOpen, London, p. 10.

[20] Valentini, D., Lorusso, A. M. and Stephan, A. (2020). "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization", *Frontiers in Psychology*, Vol. 11, March, p. 12.

[21] For example, see: Whittaker, J. (2022). *Recommendation Algorithms and Extremist Content: A Review of Empirical Evidence*, Global Internet Forum to Counter Terrorism; Yesilada, M. and S. Lewandowsky (2022). "Systematic review: YouTube recommendations and problematic content", *Internet Policy Review*, Vol. 11, Issue 1; Whittaker, J., Looney, S., Reed, A., and Votta, F. (2021). "Recommender Systems and the Amplification of Extremist Content", *Internet Policy Review*, Vol. 10, Issue 2.

[22] Valentini, D., Lorusso, A. M. and Stephan, A. (2020). "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization".

recommending more content to each other[23]. In their research on two far-right children who radicalised using gaming platforms, Koehler, Viebig, and Jugl suggest that their case studies demonstrate support for the onlife thesis, noting that "fluid interactions between [online and offline realities] in both cases were clearly visible throughout the radicalisation pathways"[24].

4. Understanding radicalisation environments

Online radicalisation is a redundant concept and, therefore, attempting to theorise or model the process is unlikely to be helpful. However, there is still value in attempting to understand how different types of communication technologies affect the radicalisation process. Gill et al. observe that rather than fixating on a specific location (such as online or offline), we should "understand the drives, needs, and forms of behaviour that led to the radicalization and attack planning and why offenders chose that environment rather than purely looking at the affordances the environment produced"[25]. The question should therefore not be: 'do terrorists radicalise online?' but rather 'what role do information environments play in radicalisation?' Attempting to dichotomise between online and offline is not only impossible, but also places a range of communications technologies in a broad category, even when there are more differences than similarities. For example, the user experience on video-streaming platform YouTube has little in common to the pseudonymous chats of Telegram or almost face-to-face experience of Zoom. Rather than grouping all of these activities together, researchers should seek specificity about the user experience and attempt to understand how the affordances interact with radicalisation processes.

Online technologies will only ever be part of the radicalisation process. Therefore, attempting to theorise or model the process of online radicalisation will always be a limited endeavour. It is more fruitful to consider a full, holistic understanding of radicalisation and if one is interested in the role of communications technologies, attempt to understand how it intersects with other important factors. Situational Action Theory (SAT) seeks to explain how an individual's norm-based motivations interact with their propensity to radicalisation. To put it simply, it asks why some people get to a point in which they see terrorism as an acceptable form of action[26]. The theory emphasises the importance of socialisation and environment, regardless of whether they take place on the Internet or face-to-face. Similarly, it does not assume that propaganda will resonate with their audience (nor does it preclude it), but rather it attempts to understand why it may resonate with some, but not others, given a range of factors[27].

Bouhana developed the 5S framework – based on SAT – which takes a systemic perspective to understanding radicalisation. The first factor is individual Susceptibility – characteristics that may predispose them to becoming radicalised. This can be exacerbated by the individual's Selection – exposure to certain people, locations or ideas; Bouhana demarcates 'social selection,' such as residence and socioeconomic status, from 'self-selection,' where individuals choose to spend their time. This is in turn affected by the different affordances that the Settings offer individuals, such as whether certain settings encourage extremism or whether they fail to discourage social or legal norms. One level up from these settings is the Social Ecology – the

[23] Whittaker, J. (2022). "Rethinking Online Radicalization", *Perspectives on Terrorism*, Vol. 16, Issue 4, pp.27-40.

[24] Koehler, D., Fiebig, V. and Jugl, I. (2022). "From Gaming to Hating: Extreme ¬ Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms", *Political Psychology*.

[25] Gill, P. et al, ibid., p. 114.

[26] Wikström, P. O. H. and N. Bouhana (2017). "Analyzing Radicalization and Terrorism: A Situational Action Theory", in LaFree, G. and Freilich, J. D. (Eds.), *The Handbook of the Criminology of Terrorism*. John Wiley & Sons, Chichester, pp. 175–186.

[27] Bouhana, N. (2019). "The Moral Ecology of Extremism: A Systemic Perspective," Commission for Countering Extremism, gov.uk/government/publications/the-moral-ecology-of-extremism-a-systemic-perspective.

communities that may support the emergence or maintenance of these affordances. Finally, the model includes the System-level factors, such as social norms, governance and strains. These system level factors play a role in the emergence of social ecologies but also affect the susceptibility of individuals.

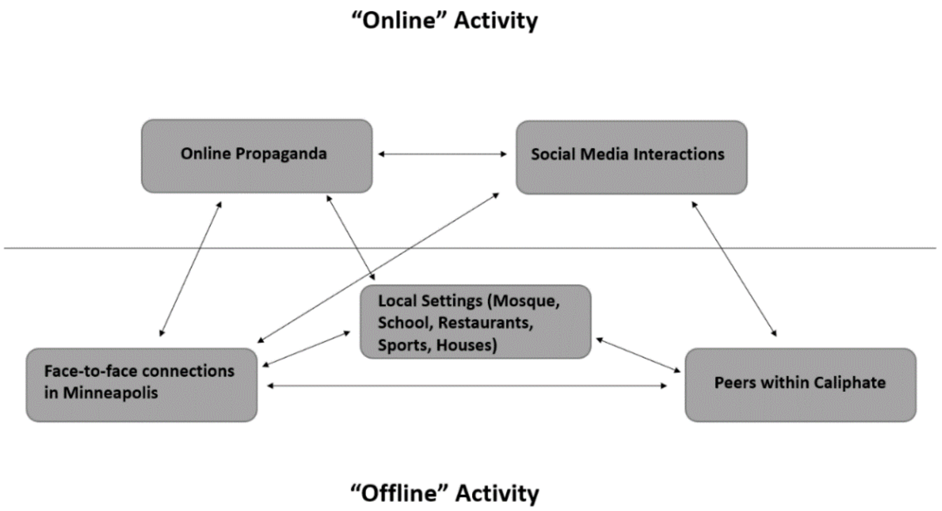
"Online" Activity
Online Propaganda
Social Media Interactions
Local Settings (Mosque, School, Restaurants, Sports, Houses)
Face-to-face connections in Minneapolis
Peers within Caliphate
"Offline" Activity

Figure 1: Yusuf's online vs offline activities

4.1 Case study: Abdullahi Yusuf

To demonstrate how a holistic radicalisation framework – such as Bouhana's 5S model – can be used to better understand actors' information environments, the following section will analyse a case study of Abdullahi Yusuf, an individual who was caught attempting to leave Minneapolis/St Paul for Syria in 2014 and subsequently convicted of conspiracy to provide material support to a foreign terrorist organisation[28]. This case study is not intended to be representative of the experiences of all terrorists – it was chosen in part because there is a large amount of open-source data on Yusuf, including several court documents and interviews with him conducted by journalists. Rather, this case was chosen for the purposes of exposition to demonstrate the limited analytic utility of an online/offline dichotomy compared to a theory which can account for the multiplicity of interrelated environments.

Yusuf was part of a deeply interconnected network in the Twin Cities who either successfully or unsuccessfully attempted to travel to join jihadist groups. This was the most active recruitment network in the USA[29], with the FBI estimating that at least 45 left the area to join foreign jihadist groups, or others, such as Yusuf, being caught by law enforcement prior to travel[30]. These individuals knew each other from their local community – they are almost all from a Somalian background – and in previous years, members of the community had left the area to fight for al-Shabaab[31]. Many of the individuals went to the same school and formed a friendship network, often playing

[28] USA v. Abdullahi Yusuf (2015). Judgment in a Criminal Case, CASE 0:15-cr-00046-MJD, United States Court for the District of Minnesota.

[29] Meleagrou-Hitchens, A., Hughes, S. and Clifford, B. (2018). "The Travelers: American Jihadists in Syria and Iraq", *Program on Extremism*.

[30] Aslanian, S., Yuen, L. and M. Ibrahim (2015). "Called to Fight: Minnesota's ISIS Recruits", *MPR News*, 25 March, mprnews.org/story/2015/03/25/minnesota-isis#yismail.

[31] Vidino, L. Harrison, S. and C. Spada (2016). "ISIS and al-Shabaab in Minnesota's Twin Cities: The American Hotbed" in Varvelli, A. (Ed.), *Jihadist Hotbeds: Understanding Local Radicalization Processes*. Italian Institute for International Political Studies, Milan.

basketball together and forming tight social bonds[32]. It was with these friends that he made the decision and planned to travel to the 'caliphate', with one giving him a 'now or never' ultimatum: "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"[33], to which he immediately agreed. Given the heavy reliance on face-to-face interactions, at first glance, this may seem like a textbook case of offline radicalisation.

Despite the clear offline elements to Yusuf's radicalisation, there are clearly key online aspects too. Yusuf watched a substantial amount of online propaganda, which he said '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"[34]. He also conducted his own 'research,' when a teacher asked him to complete a report on the war in Syria. When he learnt of the atrocities that the Assad regime were committing against Sunni Muslims, he felt a deep sense of moral outrage[35]. He also used social media platforms, his Facebook profile picture was a man depicted with a head of a lion – jihadist foreign fighters are often described as such[36] – and would post comments such as "Bashaar asad don't deserve to live"[37]. He frequented a YouTube channel called 'Enter The Truth,' which contained slick IS productions that demonised the West and highlighted Muslim suffering[38]. Yusuf described binging this channel as analogous to 'one more episode of Game of Thrones,' framing himself as a noble warrior instead of a helpless bystander[39]. His travel to Syria was also inspired by connections he had made on Instagram, having noticed fighters "having nice villas and nice cars and stuff like that"[40].

An analysis of Yusuf's case demonstrates that there are important motivators within both the online and offline domains. This is not inherently problematic; one might classify it as 'mixed' radicalisation. However, a deeper analysis demonstrates that it is difficult to classify many of the behaviours into either domain. 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. For example, Yussuf did engage heavily with online propaganda, but he often did this with his friends; they would all go to one of their homes after basketball sessions and watch YouTube together, trading mobile devices, suggesting new content to each other and discussing it amongst themselves[41]. Similarly, many of the individuals who he was interacting with online were part of his local face-to-face network as well. Some of these individuals travelled to the 'caliphate' before him and then became a point of contact for him, both inspiring to join the 'caliphate', as well as facilitating him by offering advice to Yusuf and his co-conspirators[42]. This was done via social media but was reliant on existing face-to-face connections. This is the onlife thesis in practice; activities that may at first glance appear as 'online' or 'offline' are actually not possible to demarcate.

[32] Koerner, B. I. (2017). "Can You Turn a Terrorist Back into a Citizen?", *Wired*, 28 March, wired.co.uk/article/deradicalisation-terrorism-daniel-koehler.

[33] Temple-Raston, D. (2017). "He Wanted Jihad. He Got Foucault", *New York Magazine*, 26 November, nymag.com/daily/intelligencer/2017/11/abdullahi-yusuf-isis-syria.html.

[34] Temple-Raston (2017), ibid.

[35] Koerner (2017), ibid.

[36] Benedek, E. and N. Simon (2020). "The 2017 Manchester Bombing and the British-Libyan Jihadi Nexus", *CTC Sentinel*, Vol. 13, Issue 5, pp.1-12.

[37] USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint, Case: 14-MJ-0124, United States District Court for the District of Minnesota, 2014, p.22.

[38] Koerner (2017), ibid.

[39] Temple-Raston (2017), ibid.

[40] Temple-Raston (2017), ibid.

[41] Koerner (2017), ibid.

[42] Meleagrou-Hitchens et al. (2018), ibid.

Rather, the contemporary lived experiences meshed the two inseparably, as demonstrated in Figure 2.

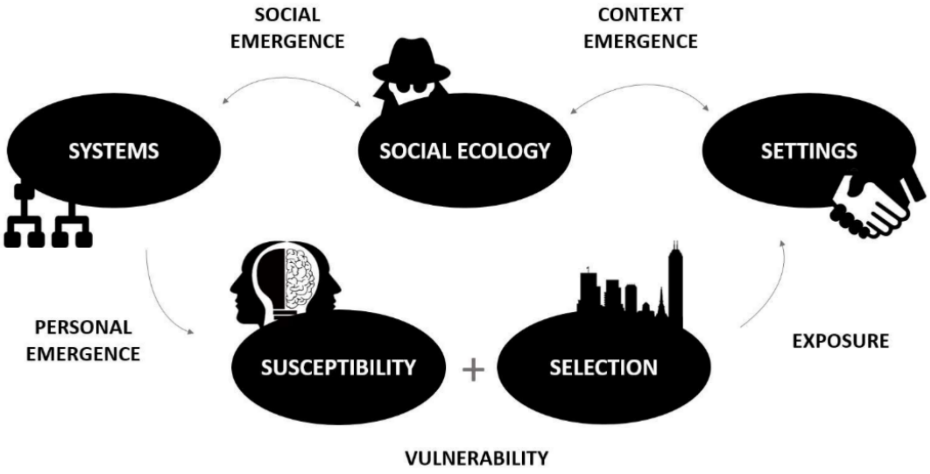

Figure 2: Bouhana's 5S framework

4.2 Using SAT to understand Yusuf's radicalisation

Given that Yusuf's activities cannot be easily demarcated into online or offline behaviours, it is more fruitful to adopt a holistic approach to radicalisation[43]. Bouhana's 5S framework, which is based on SAT, helps us identify the interplay between a range of factors that were important in Yusuf's radicalisation. When considering his Susceptibility, which is a key determinant of moral change[44], several factors are apparent within this case. He outlines a need to fulfil a sense of adventure by travelling to the 'caliphate' and thinking he was going to be part of IS' special forces[45]. This sense of adventure was, in Yusuf's own words, propelled by consuming online propaganda which fed his thrill-seeking nature. Mere susceptibility is not enough to predict engagement with extremism, however. Selection is important in understanding a would-be terrorist's information environment. This can be split into two parts: social selection is where an individual is placed socially – in this case Yusuf was in close proximity to a network of extremists, including at his school and mosque. Self-selection is where an individual chooses to spend their time. Yusuf chose to play basketball with his new network, as well as join meetings at restaurants and round his new friends' houses, but he also engaged with the same individuals using online platforms. Social and self-selection are interlinked; his choice to spend time online was informed by his peer network, which in turn was related to his location.

The next factor is the Settings that make up an individual's environment and encourage extremism. Yusuf had a range of moral affordances – opportunities to frame his extremist behaviour as morally legitimate[46] – such as his interactions with co-ideologues with whom he watched online propaganda and created a moral imperative upon him to travel, stating that he would be doing sacred work by saving women and children from the Syrian regime[47]. The 'now or never' ultimatum from his friend exacerbated this, making Yusuf feel that he could not say no, or else he would

[43] For a more detailed discussion of this case study, see: Whittaker, J. (2022). *Online radicalisation: the use of the internet by Islamic State terrorists in the US (2012-2018)*, Swansea University & Leiden University Doctoral Dissertation, scholarlypublications.universiteitleiden.nl/handle/1887/3250473.
[44] Bouhana, N. (2019), ibid.
[45] Temple-Raston (2017), ibid.
[46] Bouhana, N. (2019), ibid.
[47] Koerner (2017), ibid.

not be seen as a true believer[48]. The group also provided him with attachment affordances; a sense of brotherhood, which Yusuf said that he had longed for from an early age[49]. There was also a lack of social control that could have provided an intervention; his parents welcomed his new friends and his new found religiosity and the propaganda sessions happened at a time in which there was little regulation of content on the Internet[50].

Related is the Social Ecology – the community-level factors that permit or restrict radicalisation settings. The area was a hot spot for radicalisation, which could have created a social ecology which placed its members in a criminogenic environment that made engaging in terrorism a morally acceptable choice. Moreover, the Internet can provide an extremism facilitating ecology too, particularly given the reach of IS in the mid-2010s[51]. The final set of factors are System-level, which can promote the emergence of extremism-enabling ecologies. An example of this is discrimination, which Yusuf experienced all of his life due to his Somali heritage and Muslim background[52]. Systemic factors can lead to perceived marginalisation and feelings of insignificance, which he also described, noting that his poor upbringing made him feel that the American dream was unachievable and led him to question whether he belonged in the USA[53]. The Internet was an important aspect of this dynamic, exposing Yusuf to information about the treatment of Sunni Muslims, which led to his moral outrage[54].

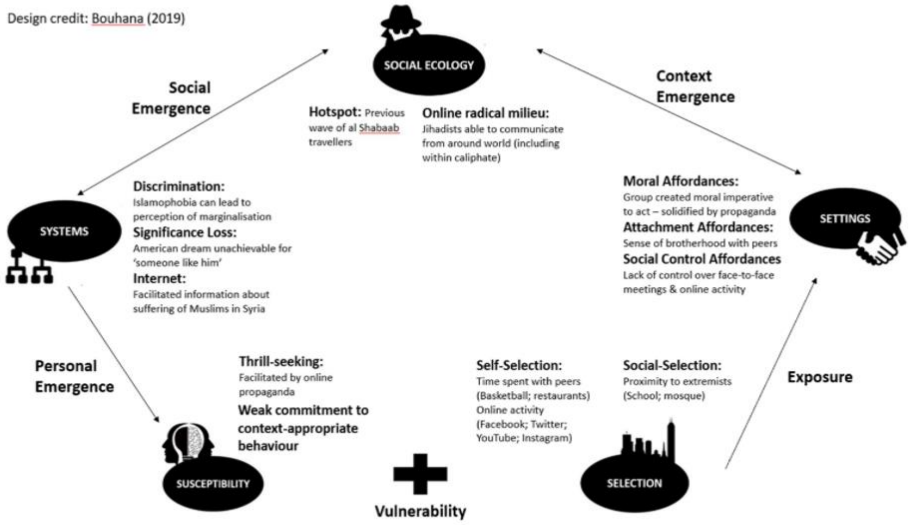
Design credit: Bouhana (2019)
SOCIAL ECOLOGY
Social Emergence
Context Emergence
Hotspot: Previous wave of al Shabaab travellers
Online radical milieu: Jihadists able to communicate from around world (including within caliphate)
SYSTEMS
Discrimination: Islamophobia can lead to perception of marginalisation
Significance Loss: American dream unachievable for 'someone like him'
Internet: Facilitated information about suffering of Muslims in Syria
SETTINGS
Moral Affordances: Group created moral imperative to act – solidified by propaganda
Attachment Affordances: Sense of brotherhood with peers
Social Control Affordances Lack of control over face-to-face meetings & online activity
Personal Emergence
Exposure
Thrill-seeking: Facilitated by online propaganda
Weak commitment to context-appropriate behaviour
Self-Selection: Time spent with peers (Basketball; restaurants) Online activity (Facebook; Twitter; YouTube; Instagram)
Social-Selection: Proximity to extremists (School; mosque)
SUSCEPTIBILITY
SELECTION
Vulnerability

Figure 3: Yusuf’s information environment, based on Bouhana’s 5S framework

Theories of online radicalisation tend to focus on how online technologies affect radicalisation. However, at both the empirical and ontological level, the online/offline dichotomy cannot withstand scrutiny. If one wishes to understand the role of technology in radicalisation, it is better to attempt to place it within a holistic

[48] Temple-Raston (2017), ibid.

[49] Temple-Raston (2017), ibid.

[50] For example see: Berger, J.M. and J. Morgan (2015). “The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter”, *The Brookings Project on U.S. Relations with the Islamic World: Analysis Paper*.

[51] Berger, J.M. and J. Morgan (2015), ibid; Carter, J., Maher, S., and P. Neumann (2014). “‘#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks”, *The International Centre for the Study of Radicalisation and Political Violence*.

[52] Koerner (2017), ibid.

[53] Temple-Raston (2017), ibid.

[54] Koerner (2017), ibid.

radicalisation framework. For this, the 5S model incorporates micro-, meso-, and macro-level factors to understand the emergence of extremist behaviours. It does not rely on an online/offline dichotomy, but rather flourishes in the complexity of the interplay between the two domains. It does not matter, for example, whether Yusuf watching propaganda on YouTube and discussing it with friends is considered an online or offline activity. Rather, the focus is ascertaining how these interactions and his wider environment affected his motivations to travel to the 'caliphate'.

5. Conclusion

This paper has sought to do three things: Firstly, to demonstrate that online radicalisation, while a popular concept, does not stand empirical or ontological scrutiny. Secondly, to argue that it is better to forgo an online/offline dichotomy when it comes to discussing radicalisation and, instead, focus on an individual's information environment, which in the contemporary world, fuses online and offline domains inseparably. Finally, by way of a case study of Abdullahi Yusuf and Bouhana's 5S framework of radicalisation, it has demonstrated the complexity of these information environments and how communications technologies can be significant at every level. Moving forward, rather than fixating on whether radicalising individuals spent more time acting online or offline, both researchers, practitioners and law enforcement can benefit from understanding an individual's propensities, selection choices and the system in which they operate and, importantly, how communications technologies interplay at each stage.

Joe Whittaker

Swansea University