ONLINE RADICALISATION

What we know

Joe Whittaker

Radicalisation Awareness Network
RAN Policy Support

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (http://www.europa.eu).

Luxembourg: Publications Office of the European Union, 2022

© European Union, 2022

The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/).This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightsholders.

TABLE OF CONTENTS

LIST OF ACRONYMS

AQ al Qaeda

EU European Union

IS The so-called "Islamic State", also known as ISIS/ISIL

LA Los Angeles, the city in California in which the 1999 attack by Buford Furrow took place

UK United Kingdom

UN United Nations

EXECUTIVE SUMMARY

Online radicalisation has become a key concern within contemporary society. Policymakers and the media have frequently framed it as a process in which individuals engage with content on the Internet and eventually become radicalised to either adopt extreme beliefs or commit violence. Researchers, while not completely rejecting this premise, have typically offered a greater degree of nuance and point to conceptual issues as well as several unanswered questions.

Extremists have been using the Internet for around three decades, if not longer. During this time, there have been frequent examples of individuals engaging heavily with the Internet and then going on to commit violent acts.

The concept of online radicalisation came to prominence around 15 years ago, with the language used to describe pathways to terrorism moving from ''root causes'' to the personal process of radicalisation.

Contemporary research repeatedly paints a complex picture. The Internet is clearly important – extremists frequently engage in a range of online behaviours – but this does not come at the expense of offline activity. Similarly, engaging with propaganda online may be a risk factor, but this is often only for individuals with certain personality traits or those that engage in specific behaviours. Several scholars have suggested that the quality of data available to understand the phenomenon is low.

The environment that a radicalising individual may find online is fundamentally different today when compared to the mid-2010s. Neither jihadists nor violent right-wing extremists enjoy the free reign in which they once did. Now, those movements face a hostile ecosystem and rely on a host of platforms such as end-to-end encrypted apps; file hosting sites; terrorist operated websites; alt-tech platforms; and the decentralised web. There has also been an increase in the use of game adjacent platforms and gamification within the extremist sphere.

Recommendation algorithms creating ''filter bubbles'' are frequently highlighted as a potential conduit of radicalisation. Research suggests that they may promote extreme content, but we know little about their role in the radicalisation process.

The COVID-19 pandemic and the extra hours spent online as a result of lockdown policies is also a cause for concern, with many suggesting that it created the 'perfect storm' for radicalisation when

combined with other factors such as uncertainty, isolation, and psychological distress. While this is a valid concern, claims that more time spent online will lead to a greater chance of radicalisation should be treated with caution. Moreover, the early data do not bear this out.

Moving forward, researchers have pointed to the metaverse as a potential for extremist exploitation in future. More broadly, as stakeholders become more adept at content removal, we should expect extremists to innovate and create ecosystems that are more security conscious. This may hamper law enforcement's ability to conduct investigations. Moreover, there may be little utility in attempting to separate the 'online' and 'offline' worlds; technological innovation has inseparably enmeshed the two. Extremists' behaviours are not easy to demarcate into one domain or the other. As we move towards the Web 3.0 and metaverse, this will only continue.

Future research should be less concerned with attempting to understand the importance of the online or offline domains, but rather, it should attempt to establish how communication technologies can interplay with different levels of radicalisation (i.e. personal, environmental, systemic). While the recent increase in experimental designs is welcome, it must begin to incorporate longitudinal designs to fully understand how extremist media affects its audience. Finally, research should aim to establish the base rates for risk indicators to understand if a radicalised population differs from the wider public.

INTRODUCTION

Over the past three decades, the Internet has gone from a fringe communication technology to ubiquitous in day-to-day life. Like the rest of us, violent extremists have used it to socialise, learn, and be activists for their cause (Neumann 2013). For around fifteen years, the idea of 'online radicalisation' has been a pressing concern within policy circles and the media, as well as receiving substantial academic interest.

For many years, scholars noted that there was a lack of data-driven research which analysed the phenomenon, instead relying on anecdotal evidence and an over-emphasis on analyses of extremist online content (Gill et al. 2015; von Behr et al. 2013). However, recent years have seen a substantial increase in empirical studies which, from different perspectives, attempt to understand the ways in which the Internet may play a role in the radicalisation process. As such, it is important to consolidate this research to comprehend what we know about the contemporary picture. This is the core objective of this report.

In presenting an updated understanding of our knowledge of online radicalisation, this report begins with a section which explores the ways in which online radicalisation is conceptualised by policymakers, the media, and researchers. This is followed by a brief history of the concept from the early years of the world wide web up to the present day, highlighting how the idea came to prominence. The third section, which makes up the majority of the report, focuses on recent research on the topic. This includes a discussion of the literature and meta-reviews on the topic; database studies which analyse violent extremists' use of the Internet; experimental studies on the effects of propaganda; the contemporary online environment that radicalising individuals may find; and research which explores whether the extra hours spent online during the COVID-19 pandemic will lead to a greater likelihood of radicalisation. It finishes with a brief reflection on how the situation may change in future. As the objective of this report is to understand what we know about contemporary online radicalisation, this section will prioritise research that has been published within the last five years (although this does not exclude older studies where still relevant). This will be followed by a conclusion which lays out the points of consensus amongst the literature and identifies the gaps in knowledge that are ripe for future research.

If there is a single key takeaway from this report, it is one of complexity. There is a substantial justification for the policy concern – research demonstrates that extremists are using the Internet to recruit and socialise, and that online propaganda may be effective in persuading its target audience. However, this research comes with equivocations. For example, offline interactions remain key in radicalisation and propaganda effects are often moderated by personality or behavioural factors. Ultimately, there are still far more questions than answers.

CONCEPTUALISING ONLINE RADICALISATION

POLICY AND MEDIA CONCERN

Online radicalisation has been repeatedly highlighted by policymakers as a key concern. Europe's core institutions, such as the Council of Europe (2014), the European Commission (2015), Europol (2020; 2021; 2022), and the Organization for Security and Co-operation in Europe (2016) have all emphasised it as a pressing security threat. In 2017, French President Emmanuel Macron and former UK Prime Minister Theresa May established the joint "French-British Action Plan" to tackle online radicalisation (HM Government 2017). This concern has also been highlighted by the Government of the United States (Wiktorowicz 2013), the FBI (nd), and the former Secretary General of the United Nations (Ki-Moon 2016).

The peak of this concern was seen during the mid-2010s when over 50,000 individuals travelled from countries around the world to join the so-called Islamic State (IS) in Syria, Iraq, and other countries (Cook and Vale 2019) The high quality 'Hollywood-esque' propaganda that was transmitted via the Internet was a critical factor in their recruitment success (Hafez and Mullins 2015; Lakomy 2017a). However, recent years have seen an increase in the online presence of several other movements, such as violent right-wing extremists (Pauwels 2021), involuntary celibates (Hoffman, Ware, and Shapiro 2020; Cottee 2020) and groups driven by conspiracy theories such as QAnon (Robertson and Amarasingam 2022).

The logic behind this concern is relatively straightforward: online extremist content (both propaganda and peer-to-peer communications) can persuade vulnerable audiences to share terrorists' worldviews, and potentially engage in violent activities. The Executive Director of Europol Catherine De Bolle notes that 'the online environment plays a key role in this as it facilitates (self-) radicalisation and the spread of terrorist propaganda' (Europol 2022, 3), while Dutch Prime Minister Mark Rutte, who endorsed the Macron/May initiative, said it was imperative to stop 'vulnerable young people from being exposed to terrorist ideologies on their smartphones and laptops and being drawn in' (Rutte 2017). Similarly, the European Commission's 2020 Counter-Terrorism Agenda notes that: 'The spread of radical ideologies and of terrorist guidance material accelerates through the use of online propaganda, with the use of social media often becoming an integral part of the attack itself' (European Commission 2020, 1), To put it simply, the Internet offers instant communication for almost no cost, which offers groups and movements the ability to market their extremist content in large quantities to audiences around the world.

This concern is often shared by the press, which frequently publishes headlines such as 'YouTube, the Great Radicalizer' (Tufekci 2018); 'Beware the Rabbit Hole of Radicalization' (Washington Post Editorial Board 2019); or 'We need to talk about the online radicalisation of young, white women' (Tait 2017). Such stories typically suggest that online platforms are playing a key role in radicalising their audiences, often by exacerbating polarisation with their sites' architecture (such as recommendation systems). Stories in the press often present this problem in an alarmist manner; for example, former right-wing extremist Caleb Cain received wide press coverage when he said:

'because of the way that propaganda works online literally anyone can become radicalised, and you don't realise that you're being groomed into a cult' (Gough 2021).

The last two years and the COVID-19 crisis has exacerbated these concerns further amongst both policymakers and news sources. They fear that the pandemic may have created a 'perfect storm' of factors – social isolation, fear of becoming ill, financial concerns, dissatisfaction with government, disinformation – which all work together with individuals' spending more time at home in front of computers, which could exacerbate radicalisation (Europol 2021). The UN Counter-Terrorism Executive Directorate mirrored this concern, warning that the lockdowns created a 'captive audience' of vulnerable individuals who were spending considerably more hours unsupervised online (UN CTED 2020). The former EU Counter-Terrorism Commissioner noted that the pandemic also revealed the nexus between illegal extremist and 'legal yet harmful' content, which he argued can be amplified by social media platforms' recommendation systems and play a role in recruiting individuals into violent movements (Council of the European Union 2020b). News organisations around the world have repeatedly run stories which express concerns about this 'perfect storm' and the possibility that it leads to an increase in extremist attitudes, or even violent behaviours (Rodriguez 2021; Wood 2021; Hurst 2022).

It should be clear that the policy position is not that they believe that the Internet is the only, or even primary, concern when it comes to radicalisation. There are hundreds of offline initiatives that are developed to attempt to curb violent extremism. The *Radicalisation Awareness Network* documents several hundred existing practices including early prevention; exit strategies; community engagement; education; family support; and prison interventions (RAN, 2021). However, as this section has demonstrated, policymakers are deeply concerned with the idea that access to extreme content online plays a key role in contemporary radicalisation.

ACADEMIC CONCEPTUALISATION

Despite the wide-ranging concern from policy and media circles, researchers have highlighted several conceptual issues surrounding online radicalisation. Macdonald and Whittaker (2019) note that it is unclear what constitutes enough online activity to be classified as 'online radicalisation.' They also highlight three phrases related to the phenomenon that are ambiguous. First, it is often not clear what constitutes 'radicalisation' – for some it is a cognitive process which ends with an individual developing extreme beliefs, while for some it is a behavioural process which ends with violent actions – an argument made by several other scholars (Schuurman and Taylor 2018; Borum 2011; Horgan 2008). Second, they argue that the phrase 'self-radicalisation' (often, but not always, used interchangeably with 'online radicalisation') is a redundant concept because it overlooks the social nature of the Internet, which is a point also made by Conway (2017). Third, they note that the term 'echo chamber' – also rarely defined and conceptually ambiguous – is frequently posited as a key mechanism of the process, but that this relationship is not supported by empirical evidence (Whittaker 2020). Macdonald and Whittaker (2019) argue that this conceptual ambiguity leads to an array of problems: it can lead to internal incoherence which affects the robustness of research; it makes synthesising knowledge in the form of meta-reviews more difficult; and it makes it more difficult to communicate research findings to interested audiences, such as policymakers or the media. Meleagrou-Hitchens and Kaderbhai offer a reasonable summary of the concept amongst researchers: 'there is little agreement on what constitutes online radicalisation and how, if at all, it happens' (Meleagrou-Hitchens and Kaderbhai 2017, 17).

To elucidate this conceptual ambiguity, one should consider the different ways in which the process is framed. For some, like Sageman (2008) it is described as a replacement or alternative for offline radicalisation, while Bermingham et al. (2009) and Neumann (2013) it relates to the radicalising effects that specific online interaction and exposure may have on their audience. Whittaker (2022a) takes a differing view and is more concerned with specific violent extremist behaviours and how they manifest on the Internet. Others have conceptualised the process as acted *exclusively* in the online domain – i.e. no interactions with the radical milieu offline at all (Pearson, 2016), while for others it is about where the individual spent most of their time (Hamid and Ariza, 2022; Kenyon,

Binder, and Baker-Beall, 2022) A study by von Behr et al. (2013) broke the process down into 5 testable hypotheses:

1. The Internet creates more opportunities to become radicalised
2. The Internet acts as an 'echo chamber'
3. The Internet accelerates the process of radicalisation
4. The Internet allows radicalisation to occur without physical contact
5. The Internet creates opportunities for self-radicalisation

Attempting to find academic consensus as to what constitutes "online radicalisation" is an impossible task. Some researchers set such a high bar of "online only" that it describes only few individuals, while others are more concerned with where violent extremists spend *most* of their time, while others are more concerned with the effects that the Internet has on its audience. As such, the research outlined below will attempt to deal with the conceptual ambiguity by being as specific as possible about the phenomenon under study, rather than attempting to focus on one common understanding.

There are typically two camps of researchers' conceptualisation of the role of the Internet in radicalisation. The first, which mirrors that of policymakers and the media, suggests that it plays a very important role. Weimann (2012) suggests that the Internet era was a 'paradigm shift' which changed the nature of terrorism from groups congregating and plotting in physical spaces to the promotion of lone actor attacks: 'The real threat now comes from the single individual, the 'lone wolf', living next door, radicalized on the internet, and plotting strikes in the dark' (Weimann 2012, 75). This argument is also proffered by Post, McGinnis, and Moody (2014) who suggest that the Internet created a host of 'lone wolf terrorists who, through the Internet, are radicalized and feel they belong to the virtual community of hatred' (Post, McGinnis, and Moody 2014, 306). Famously, Sageman suggested that by the mid-2000s, 'face-to-face radicalisation has been replaced by online radicalisation' (Sageman 2008, 41).

Although many of these views dominated research in the 2000s and early 2010s, most contemporary scholars take a more sceptical tone. Glazzard (2019) notes that the Internet is clearly important but downplays the policy and media concern. Terrorists and extremists use the Internet for a range of activities including propaganda dissemination, planning activities, and post-event communications. However, to blame the Internet is to 'shoot the messenger.' He argues that the Internet may facilitate terrorism but does not cause it. It is this latter, and more nuanced view, which is held by most scholars today, as noted in a literature review on the topic of online radicalisation carried out by Meleagrou-Hitchens and Kaderbhai:

> There is at least broad consensus that the Internet alone is not generally a cause of radicalisation, but can act as a facilitator and catalyser of an individual's trajectory towards violent political acts. Use of empirical evidence to draw convincing conclusions remains scarce, and this has greatly impacted on the strength of research on this topic (Meleagrou-Hitchens and Kaderbhai 2017, 17)

Hitchens and Kaderbhai note that scholars tend to take a more sceptical tone than the views laid out by policymakers and the media above. Rather, while understanding its importance, they stress that the relationship is complex with many gaps in knowledge.

HISTORY OF ONLINE RADICALISATION

ORIGINS

The age of the Internet has precipitated a communications revolution and has become ubiquitous around the world. Originally conceived as a US Government project in the 1960s, it underwent several iterations before Tim Berners Lee wrote the first web browser in the mid-1990s (Bartlett 2015). Since then, it has fundamentally changed day-to-day life; in 1995, there were 16 million web users, whereas today there are over 5 billion, representing 63 % of the world's population (Datareportal 2022). In the EU, this is much higher; the *Digital Economy and Society Index* notes that 92 % of households had a subscription to the Internet in 2021 with 87 % of people using the Internet regularly (European Commission 2022).

Given this momentous rise over the past three decades, it is unsurprising that terrorists and extremists have also turned to the web, particularly given that they have typically been early adopters of new technologies (UN CTED 2015; Bloom, Tiflati, and Horgan 2017; Levin 2015). In 1995, Don Black, former Grand Wizard of the Ku Klux Klan and member of the American Nazi Party, created the online forum Stormfront, which remains active to this day, and presently has over 370,000 members. After creating the platform, Black noted: 'The Internet is the opportunity we've been looking for…We were never able to reach an audience that we can now [reach] so easily and so inexpensively' (Black, quoted in: Cohen-Almagor 2014, 432).

By 1999, researchers had begun to take note of how terrorists were using the Internet, with groups exploiting the ability to reach unprecedented audiences to spread propaganda, coordinate plans, and finance plots (Arquilla, Ronfeldt, and Zaini 1999). Conway (2002) also warned that the Internet was becoming a substantial security threat, being used for far more than operational support. Rather, it represented a political power shift as it was the first 'many to many' communications system which underlies the power to persuade, inform, witness, debate, and discuss, while cutting out traditional gatekeepers such as news organisations. By the mid-2000s, Weimann (2004) observed that all active terrorist groups had established a presence online. He notes eight ways in which terrorists were using the Internet psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilisation, networking, sharing information, and planning and coordination. Sageman (2004) also warned about the exploitation of the Internet and how it could affect the future of recruitment, arguing that it could create a strong bond between an individual and their online community due to the immediate responses in chat rooms; a lack of moderating voices; and a prevalence towards simple ideological solutions. Within these early years, research also highlighted several case studies of terrorists who had used the Internet heavily as part of their plots. These include Buford Furrow, who attacked the L.A. Jewish Community Center in 1999 after using the web to gain both inspirational and instructional information (Levin 2002) and David Copeland who conducted a series of nail-bomb attacks in London in the same year having used the Internet for various aspects of his plot (Back 2002).

'ONLINE RADICALISATION' AND MOVING INTO THE 2010S

It was not until the latter half of the 2000s that the notion of 'online radicalisation' came to prominence in policy and research circles. This is because the word 'radicalisation' had not been particularly prevalent until after the London bombings of 7 July 2005 (Sedgwick 2010). Prior to this, research had been focused on 'root causes' of terrorism – i.e. the conditions in society or an individual that may trigger or act as a catalyst for violence (Horgan 2008). In a literature review of 200 articles which include the term 'online radicalisation', the first returned publication date was 2006 (Gill et al. 2015). This is a subtle, yet important difference in framing. Previous research had explored the ways in which terrorists had used the Internet, but by switching focus to a process (i.e.

the '*isation*') and attempting to understand how online activity affects individuals in terms of radicalising, it implicitly creates a cause-and-effect problem to be solved. After this point, research which posits the Internet as an important, and sometimes key, factor became prevalent (For example, see: Ryan 2007; O'Rourke 2007).

The combination of the events of 9/11 in the US, which pushed terrorism to the top of the global security agenda, and the prodigious rise of the Internet in the early 2000s, meant that online jihadist radicalisation became a political priority. Often, this was framed as young individuals who were part of a disaffected Muslim diaspora who accessed the Internet to join extremist communities that offered them acceptance (Post, McGinnis, and Moody 2014). The radical preacher Anwar al-Awlaki was often posited as a propagandist who could motivate Western audiences:

> For a generation of Western Muslim youth looking for easy answers to complex questions (often via the Internet), Awlaki helped find a way for the global jihad movement to appeal to many who may otherwise have been beyond its ideological reach (Meleagrou-Hitchens 2020, 168)

In the early 2010s, the prime security threat turned towards IS. As noted above, over 50,000 individuals travelled to join the group, with IS plotting and inspiring hundreds of attacks. Moreover, the group maintained a strong presence on social media; there were judged to be at least 46,000 IS-supporting accounts on Twitter (Berger and Morgan 2015) and thousands of foreign terrorist fighters beamed their lives in real time back to friends and family around the world (Klausen 2015), often with the help of supporters disseminating the content widely (Carter, Maher, and Neumann 2014). This mobilisation, combined with the group's reach on social media and their slick propaganda, led to a widespread concern about the role of the Internet in radicalisation – UN Security Council Resolution 2178 explicitly required states to take steps to address this threat and included a section which expressed concern over the role of the Internet 'to incite others to commit terrorist acts' (United Nations Security Council 2014, 1).

While IS was occupying headlines around the world, the threat from violent right-wing extremists did not go away and in recent years has seen a strong resurgence, particularly in an online context. Scrivens et al. (2022) highlight several terrorist attacks over the last five years in which the Internet played an important role, including the vehicle borne attack in Charlottesville in 2017; and the Christchurch, El Paso, and Halle attacks in 2019, Buffalo and Bratislava in 2022 During these years, violent right-wing extremists grew and maintained a substantial online presence. For example, Atomwaffen Division – a neo-Nazi accelerationist movement made up of a range of cells in America, Europe, and elsewhere – emerged from the *Iron March* forum. Like IS, it rose to notoriety 'because of its impressive and highly sophisticated propaganda operation, spearheaded by well-produced videos of the group's 'hate camp[s]'… in the American wilderness' (Ware 2020, 83).

CONCEMPORARY ONLINE RADICALISATION

LITERATURE AND SYSTEMATIC REVIEWS

One of the most fruitful ways of understanding the current state of knowledge on any topic is to synthesise the existing research. This has been done several times in recent years on the topic of online radicalisation; reviews have taken a macro view of the field and summarised the corpus of studies. Looking at these studies, three themes emerge: That there is no causal connection between using the Internet and becoming radicalised; online activity as a potential risk factor; and there being a lack of rich data to fully understand the phenomenon.

A - No Causal Connection

Meleagrou-Hitchens and Kaderbhai (2017) surveyed the literature from 2006-2017, suggesting that the main point of consensus was that the Internet offered a range of advantages to terrorists, including having access to radicalising propaganda. However, they note that for this period, the case for a causal connection between engaging with these materials and committing violent acts has not yet been made. Similarly, they play down the possibility of 'online only' radicalisation, instead highlighting that most scholars take a nuanced position that 'asserts the importance of online influences without negating the requirement of offline interactions' (Meleagrou-Hitchens and Kaderbhai 2017, 36). A similarly nuanced view is taken by Winter and colleagues, who note that 'most scholars agree that the Internet does not cause radicalisation…it is usually taken as a given that online processes, interactions, and activities complement but do not substitute their offline counterparts' (Winter et al. 2020, 10).

There have also been recent literature reviews that have looked specifically at violent right-wing radicalisation online. This is timely because much of the research that analyses terrorist behaviours has been focused on jihadism. Marwick and colleagues come to similar conclusions of many of the meta-reviews discussed above, noting that: 'The internet does not cause radicalization, but it helps spread extremist ideas, enables people interested in these ideas to form communities, and mainstreams conspiracy theories and distrust in institutions' (Marwick, Clancy, and Furl 2022, 2). Similarly, Scrivens et al. (2022) survey the existing literature to establish five core functions in which the movement uses the Internet, based on a framework created by Conway (2006): information provision; networking; recruitment; financing; and information gathering. Relevant to this topic, they find that they have been able to spread propaganda and beef up networks across a range of different platforms, both mainstream and fringe. Importantly, they highlight how little is known about the link between the online and offline worlds of extremists. Both pieces of research highlight, like many of the scholars, that extremists use the Internet heavily, but there is a lack of evidence to suggest that this is at the expense of offline interactions.

B - Online activity as a risk factor

Looking at the effects of different types of media on radicalisation, Wolfowicz, Hasisi, and Weisburd (2022) conduct a systematic review,[1] synthesising the effects of 23 media-related risk factors[2] to assess how they affect either cognitive (developing extreme beliefs) or behavioural (engagement in violent behaviours) radicalisation. They suggest that there are somewhat mixed results when it comes to the present state of knowledge. Regarding cognitive radicalisation, they find that even the most salient factors are relatively weak when compared to other (non-media) risk factors. On the other hand, engaging with online extremist propaganda (both actively and passively) did produce robust estimates for behavioural radicalisation. They conclude that these findings may support policymakers' concerns about the role of the Internet in radicalisation, but offer a cautionary note that the quality of evidence is low and that many of the studies suffered from bias, which they suggest is a reason to interpret the findings with caution.

Hassan et al. (2018) conduct a similar study to Wolfowicz, Hasisi, and Weisburd (2022), attempting to ascertain whether the Internet may act as a space which is favourable to radicalisation.[3] They find that there is tentative evidence that radical online content is associated with both online and

[1] The Review consisted of 53 studies from 2002-2020, four of which used experimental methods and 49 were experimental.

[2] These risk factors include: Active engagement with radical content; Willingness to carry out an ideologically motivated cyber attack; Being a victim of cyber bullying; participating in online discussion forums; Frequency of Facebook usage; Internet usage to follow politics; Exposure to mixed forms of media for news/violent content; Engagement in ideologically motivated hacking; Access to the Internet; Following terrorist groups' news sources; level of attachment to online networks; reading a printed or online newspaper; passive exposure to radical content; illegal downloading of content from the Internet; posting political views/opinions online; listening to the radio; self-censorship; digital literacy; watching television; time spent on the Internet; trust in media; frequency of Twitter usage.

[3] They survey 5,182 studies, finding only 11 that meet the appropriate methodological rigour for inclusion.

offline extremism, particularly for individuals that are actively seeking such content. However, they note there is no clear support for the idea that individuals radicalise online independently of offline factors; they summarise the evidence as the role of the Internet being one of decision-shaping, which in association with offline factors, can facilitate decision-making.

C - A Lack of Rich Data

One theme that frequently emerges within the academic literature is the lack of rich data, robust methods, or conceptual clarity when thinking about online radicalisation. As noted above, Wolfowicz, Hasisi, and Weisburd (2022) note that the field of propaganda effects suffers from biased studies. Hassan et al. (2018) highlight a range of limitations that are not acknowledged by authors, including retrospective or cross-sectional designs which makes the direction of effects impossible to determine; the use of self-report data; a reliance on small samples that are generated from snowballing or self-selection; and a lack of baseline measures or comparison groups.

In a literature review conducted by Odağ, Leiser, and Boehnke (2020), they note that there is an abundance of research in the field which analyses propaganda, but that there is little focus on the actual audience. They also note that little is known about the psychological dimensions and why users are motivated to visit specific platforms, as well as the types of users and their characteristics. They argue that the literature lacks causal theories that could explain the relationship between radicalisation and the Internet from a media effects point of view. The problem of an over-emphasis of analyses on radical content is also highlighted by Whittaker (2022a). Although he highlights a growing body of literature which assesses how terrorists actually use the Internet, this body remains small and therefore we cannot be confident in many conclusions as they pertain to online radicalisation. He draws on arguments made by von Behr et al. (2013), Sageman (2014), and Aly (2017), who all argue that this discrepancy leads to a tendency to inflate the importance of engaging with radical materials online as if they were a 'hypodermic needle' or 'magic bullet' which will necessarily have a radicalising effect on their audience.

DATABASE STUDIES

As noted above by Whittaker (2022a), one of the key ways to develop a better understanding of online radicalisation is to focus less on the supply of content available to would-be terrorists, and more on actual behaviours, or as Ducol (2015) succinctly puts it, to avoid the question of 'what does the Internet do to people?' and instead ask 'what do people do with the Internet?' One important point to consider is that there are several different "terrorist" or "violent extremist" roles and outcomes that are analysed within these studies. For example, some studies look specifically at those that plotted (both successfully and unsuccessfully) attacks (e.g. Hamid and Ariza, 2022), while others include only those convicted of terrorist attacks (e.g. Gill et al. 2017). Some focus exclusively on foreign terrorist fighters (e.g. Reynolds and Hafez, 2019), while others include a mix of attackers, travellers, and facilitators (e.g. Whittaker, 2021). Research has often treated the notion of a "terrorist" (or violent extremist) in an aggregated fashion, failing 'to acknowledge that being a bomb-maker may be different than being a bomb-planter; that being a foreign fighter may differ from being a terrorist attacking the homeland; that being a terrorist financier may be different than being a gunman' (Corner, Gill, and Mason, 2016, 560). When considering online radicalisation, it may be that the Internet-based activity is differently suited for different roles – for example, it is plausible that those travelling to Syria needed to rely on online networks to a greater extent than lone actors who plotted simple attacks in their own country.

Gill et al. (2017) seek to disaggregate the concept of online radicalisation into a set of observable behaviours, such as engaging in an online network and learning about their event online.[4] They find that over half used the Internet for activities relating to their plot; importantly, when the date range

[4] Their sample includes 223 UK-based individuals convicted of terrorism between 1995-2015.

is narrowed to 2012-2015, that number rises to over three quarters. Despite this heavy Internet usage, they find that terrorists regularly engage in both the online and offline domains. This downplays the idea that the Internet has – as noted by Sageman 2008b above – replaced face-to-face Interactions as the primary domain for radicalisation. These findings are mirrored in a similar study conducted by Gill and Corner (2015) on UK and US lone actor terrorists. Again, they find heavy Internet use across a range of behaviours, but that this did not come at the expense of offline interactions. Both studies conclude that online radicalisation is a false dichotomy, and that it is more important to think about the drives, needs and forms of behaviour that led to it, rather than the domain in which it occurred.

This approach is mirrored by Whittaker (2021) who uses a similar coding system to Gill et al. (2017) to disaggregate online radicalisation behaviours.[5] He finds use of the Internet to be heavy – 92 % used it to either network or plan their terrorist activity. This includes interacting with like-minded people online, accessing propaganda, or planning their activity. However, like Gill et al. (2017), he finds that those that interacted online were significantly more likely to do so offline. In other words, face-to-face interactions were still key; terrorists were accessing the Internet as part of their plot, but were supplementing it with offline conversations and meetings with like-minded peers. This work is expanded upon by Herath and Whittaker (2021) who perform a cluster analysis on the same dataset to derive typologies of online radicalisation. They find four different pathways that contain varying combinations of behaviours:

> ***Integrated****:* Highly networked online *and* offline, while also using the Internet heavily for planning.
>
> ***Encouraged***: Heavy Internet usage for networking and planning. Did maintain a physical offline network or attended group meetings but typically did so less than the *Integrated* Pathway.
>
> ***Isolated:*** Little interaction with co-ideologues in either online or offline domain. Many still used the Internet to plan their activities, while others conducted spur of the moment attacks.
>
> ***Enclosed:*** Greater offline network connectivity than online, but still used the Internet to plan.

Herath and Whittaker (2021) argue that these findings challenge the concept of online radicalisation. Rather, their typographies all exist somewhere in the middle of a spectrum of behaviours and fixating on the polar ends will over-simplify the complex process of radicalisation.

In research analysing the behaviours of 439 terrorists in eight countries,[6] Hamid and Ariza (2022) find that the majority (238) could be categorised as having been radicalised 'mostly offline'.[7] Conversely, they judge that 77 engaged 'mostly online',[8] 40 were a mix of both,[9] while only eight could be described as 'online asocial radicalisation.'[10] Similarly to Whittaker (2021), they find that individuals who engage mostly offline were significantly more likely to succeed than those that act using the Internet. Kenyon, Binder, and Baker-Beall (2022) use a similar coding system with regard to 235 convicted UK terrorists, finding that the majority (113) could be described as 'hybrid' radicalisation, while 93 were 'face-to-face', and only 29 fulfilling the criteria of 'online.' They find that the importance of the Internet has increased over time, but that it has not replaced offline

---

[5] His sample include 231 terrorists that operated in the US on behalf of IS from 2012-2020.

[6] Their sample included individuals from Australia, Austria, Belgium, France, Germany, Spain, the United Kingdom, and the United States from 2014-2021.

[7] They describe this code as: "The individual appeared to have been radicalised outside the online world, in contact with siblings, relatives, friends, recruiters or like-minded individuals in mosques, prisons or other offline settings."

[8] "The individual appeared to have been radicalised in the online world, in contact with like-minded individuals on apps such as Telegram and/or with the mentorship or guidance of a recruiter in an online setting"

[9] "Both the offline and online world appeared to have played a significant role in radicalising the individual, as he/she had relevant offline and online connections that overlapped over time"

[10] "The individual had no online or offline social connections and had seemingly been radicalised by exposure to propaganda on the Internet. Individuals were coded as being online asocially radicalised only when the respective authorities have publicly described them as such"

interactions in importance, supporting the findings of Gill et al. (2017) and Whittaker (2021). This finding is also supported by research on US extremists by Jensen et al. (2018), who find a steady increase in Internet usage between 2005 (8 %) and 2016 (87 %), also noting that that 77 % used it to supplement (rather than replace) offline interactions.

In research conducted on 99 German foreign fighters, Reynolds and Hafez (2019) find that the geographical distribution of travellers does not support an 'online radicalisation' hypothesis, but rather clusters around pre-existing radical networks in specific regions, which supports the idea that they were radicalised offline. Bastug, Douai, and Akca (2018) find that the Internet is used heavily by at least 41 % of Canadian foreign fighters, and played some role in 76 % of cases, although they did not compare online and face-to-face activity.

EXPERIMENTAL STUDIES

Previously, there was an over-reliance on the analysis of radical content and an assumption that it would necessarily influence its audience, with limited evidence being proposed to support this assumption (Sageman 2014; Aly 2017; Odağ, Leiser, and Boehnke 2020). As highlighted above, Wolfowicz, Hasisi, and Weisburd (2022) conducted a review of studies from 2002-2020, which reported mixed results, though they did set out some evidence to support the notion that engaging with such content may constitute a risk factor for behavioural radicalisation. Since the end of their data collection process, there have been more high-quality experimental studies undertaken which have sought to understand how radical content may affect its audience.

Braddock, Schumann et al. (2022) conducted an experiment on 268 participants to test whether a specific set of personality traits known as the 'dark tetrad' – narcissism, Machiavellianism, subclinical psychopathy, and everyday sadism – play a role in an individual's likelihood to be persuaded by propaganda. They find that only Machiavellianism, and not the other three traits predict persuasion, which they suggest demonstrates the risk in assuming that propaganda will be universally persuasive, instead pointing to the importance of individual characteristics. Braddock, Hughes, et al. (2022) seek to establish whether subversive online activity, such as being abusive or harassing others, is associated with being persuaded by propaganda. They conducted two experiments in which 404 participants were shown scientific racism materials and 396 male supremacist content. Both experiments reported near identical results: if individuals engaged in subversive online activity, they were more likely to feel gratification, attribute credibility, support the propaganda's source, and be less likely to resist psychologically. They suggest that this may be problematic when it comes to radicalisation because many online platforms that host this type of propaganda also promote subversive online activity. Taken together, both studies demonstrate that extremist propaganda can be effective in persuading its audience, but everyone is not equally susceptible.

ONLINE ENVIRONMENT

The environment in which terrorists inhabit online has changed substantially in recent years. In the first half of the 2010s many major platforms took a light touch approach to the removal of content, which led to jihadists and violent right-wing extremists being able to disseminate their content with much greater reach, as discussed above. However, around 2016, platforms began to take a more proactive approach to the removal of content, when it could be identified as affiliated to a terrorist group (Conway 2016). For groups like IS, this severely undermined their ability to disseminate propaganda and network. On Twitter, the number of discoverable supporting accounts went from the high tens of thousands to the low thousands (Berger and Perez 2016), while 65 % of accounts were suspended within 70 days (Conway et al. 2018), and the accounts that did manage to disseminate propaganda had been recently set up and had few followers (Grinnell, Macdonald, and Mair 2017; Grinnell et al. 2018). This led to the group moving to end-to-end encrypted platforms, such as Telegram, which offered users greater longevity online and more operational security, although with diminished reach (Prucha 2016; Clifford and Powell 2019). During this period, right-

wing extremists did not experience the same level of disruption, Conway (2020) argues, because of the movement's fluid structure; the appropriation of meme culture and its proximity to mainstream political speech which tech companies are averse to removing, although the designation and proscription of a small number of violent right-wing extremist groups has created a mechanism by which content can be more easily referred by stakeholders (Tech Against Terrorism 2021a).

Today, the online environment reflects this hostile ecosystem for jihadists. Fisher, Prucha, and Winterbotham (2019) outline how contemporary supporters use online platforms in an attempt to avoid detection or suspension: They use 'beacons', such as Facebook, Twitter, and Telegram, which direct users to 'content stores', like archieve.org and YouTube, which are supplemented by 'aggregators' which collect a range of links to different materials around the web and store them on Facebook pages or websites. Tech Against Terrorism (2021a) identifiesies 13 categories of platforms that are used in this process, with file sharing, archiving, and video sharing sites being the most frequently used, though link shortening, audio sharing, and instant messenger services are also included. In 2020, their Terrorism Content Analytics Platform sent 10,959 alerts concerning jihadist content to various tech platforms, resulting in a 94 % removal rate. Conway, Watkin, and Looney (2022) note that all jihadist groups suffer from substantial network disruption, but maintain their presence on Telegram and decentralised platform RocketChat. The benefit of decentralisation is that the platform is not controlled by a single organisation. In this regard, users operate independently which makes the removal of content more difficult. Europol (2022) highlight several such platforms, which IS exploit to disseminate content, including microblogging site Ignite and video platform DTube. Conway, Watkin, and Looney (2022) also highlight the tactic of 'online raids' in which supporters flood comments sections of public pages with terrorist content.

In recent years, the ecosystem has become more hostile for right-wing extremists as they have been suspended from larger platforms at a greater rate. This has caused them to take to fringe and decentralised platforms. Tech Against Terrorism (2021b) note that right-wing extremist actors have been migrating to 'niche, alt-tech' platforms which champion themselves as bastions of free speech and provide a home to actors that have been removed from mainstream platforms; for example, Gab (Nouri, Lorenzo-Dus, and Watkin 2019). Baele, Brace, and Coan (2020) create a framework to better understand the dynamic and rapidly evolving extreme right-wing ecosystem. In an example of platforms that appeared more than 10 times on 8chan/pol, they find dozens of sites, including mainstream social networks; mainstream and fringe news; archiving services; content hosting platforms, and right-wing extremist websites. Macdonald et al. (2022) conducted an exploratory analysis of German and French ecosystems using Twitter outlinks as a jumping off point. Concurring with Baele, Brace, and Coan (2020), they find a host of categories of platforms being used, including all those outlined above. In particular, they note that mainstream platforms are the most frequently linked, with YouTube the most popular platform. Importantly, Tech Against Terrorism (2021a) find a substantially lower removal rate for flagged right-wing terrorist content at 50 %, compared to 94 % for jihadist content on the thirteen categories of platforms (including file sharing, archiving, and video sharing sites). Within this wide right-wing extremist ecosystem, Conway, Watkin, and Looney (2022) suggest that Telegram is still a key player; the platform continues to host groups and channels associated with several proscribed terrorist organisations, such as Atomwaffen Division and Proud Boys.

WEBSITES

As highlighted above, terrorist operated websites are a key part of the terrorist online ecosystem. Tech Against Terrorism (2022) identified and analysed 198 websites belonging to right-wing terrorists (101); Sunni, (79) and Shia (18) jihadists. From a representative sample of 33 sites, they found that almost every site incorporated audio/visual propaganda; while the majority was archived content and included a communication feature. Alarmingly, the average monthly number of visits was 1.54 million. Conway and Looney (2022) use eight case studies to demonstrate the breadth and use of terrorist websites, including those of Hamas, the Taliban, Nordic Resistance, PKK, and IS. They find that, as well as being used for the dissemination of ideological content, five of the eight had crowdfunding applications. Both Tech Against Terrorism (2022) and Conway and

Looney (2022) agree that websites pose a range of threats that demarcate them from other types of content. These include the fact that platforms are indexed on public search engines; the difficulty of removing them; and the greater control that groups have over their messages. Europol (2022) also highlight dedicated websites as a key part of the online terrorist ecosystem as they play a major role in the dissemination of propaganda.

GAMES AND 'GAMIFICATION'

Another key policy concern within the EU has been the intersection between video games and radicalisation. The use of games is not new; extremist groups have been creating and appropriating games for over 20 years (Robinson and Whittaker 2021; Selepak 2010; Lakomy 2017b). However, multiple recent terror attacks with strong links to games have increased this concern. The former EU Counter-Terrorism Coordinator Gilles de Kerchove suggests that games and gaming platforms have a strong social media dimension, which can be used to recruit and radicalise a huge, young, and vulnerable target audience (Council of the European Union 2020a). Most scholars take the view that in the rare circumstance that violent extremist organisations create their own games, it is not with a view to recruit new members, but rather to solidify the ideology and give a "green light" to individuals that are already involved in the movement to commit violence (Robinson and Whittaker 2021).

Despite this lack of direct recruitment, there is a wider concern that game adjacent platforms are being exploited by violent extremists. Analysing four of these – Steam, Discord, Twitch, and DLive – Davey (2021) identifies a wide range of right-wing extremist activity across these platforms, including support on Discord for proscribed terrorist organisations Atomwaffen Division and Sonnenkrieg Division. Importantly, however, he does not find there to be direct evidence of a concerted strategy to radicalise and recruit new individuals, but rather that gaming can act as a link for bringing together already radicalised individuals. This is echoed by Gallagher et al. (2021), who in their analysis of Discord find it to be a hub for socialising and community building, although they do point to the disturbingly young age of users on the platform. While agreeing with this analysis, Lakhani (2022) notes that the absence of evidence does not mean no radicalisation takes place and the proliferation of content on such platforms is a cause for concern.

In a rare, closed source study of two radicalised children, Koehler, Fiebig, and Jugl (2022) find that both entered the radical milieu via video games and platforms, Roblox and Discord, which led to swift influence being exerted by right-wing extremists which led to illegal offline behaviours. However, they note that their findings concur with Davey (2021) – there was no evidence to suggest extremists were utilising games to directly recruit, but rather gaming environments act as a space in which people can meet and exchange ideas. They also play down the idea that young people were being lured into such spaces, finding that they were active participants in the process. Finally, they outline a host of push and pull factors that were present, beyond acting online in such communities, including parental neglect, conflict, lack of social integration, bullying, and a desire for social status. Based on these children's own words, these offline factors played an important role in their decision to immerse themselves in radical online communities, which highlights the inseparable nature of contemporary communication technologies (Valentini, Lorusso, and Stephan 2020).

One salient aspect of the intersection of gaming and radicalisation is 'gamification' – when individuals bring elements of games into non-game contexts (Schlegel 2020). One way of conceptualising the role of gamification it is being propagated by extremist organisations or if they are being propagated in an unstructured, low-level manner. Schlegel (2021), borrowing an analogy from the famous debate between Marc Sageman and Bruce Hoffman, uses a "top down" vs "bottom up" demarcation to highlight this difference. The former relates to the strategic use of gamification, such as rankings or badges on online forums such as Patriot Peer. She argues that there are five dynamics in gamification that could play a role in the radicalisation process: Pleasure, positive reinforcement, empowerment, competition, and social relatedness. However, she does

caveat her research by asserting that the evidence base for the gamification of radicalization is small and not easy to test empirically.

There have been several examples of "bottom-up" gamification in recent years. There have been multiple terror attacks adopt game-like perspectives. Lakhani and Wiedlitzka (2022) outline several ways in which the Christchurch assailant 'gamified' the attack in 2019, including by live streaming it on Facebook in a way that resembles a 'First Person Shooter' (FPS) perspective and using gaming terminology in his manifesto. This approach was mirrored by the Halle shooter in 2019, who also live-streamed the attack – this time on Twitch, but also included an 'achievement list' in one of his documents, as well as using gaming terminology (Thorleifsson and Duker 2021). Most recently, the 2022 attack in Buffalo, NY, also live-streamed the attack on Twitch 'because only boomers actually have a Facebook account' (Amarasingam, Argentino, and Macklin 2022, 5), mirroring the visual aesthetic of the Christchurch attack. It should be noted that Twitch claim to have acted quickly to supress the live-stream, stopping it 40 seconds after it began (Lamphere-Englund and White 2022). Terrorist groups and their supporters have also adopted 'gamification' in propaganda; IS have used the FPS perspective in photo reportages in Yemen (Lakomy 2017a), while Dauber et al. (2019) highlight the appropriation of Call of Duty aesthetics in visual propaganda. Taken together, Schlegel (2021) correctly asserts that 'gamification' has become a key part of extremists' toolbelts, but also warns that because this is a nascent field of research, the evidence is limited, incomplete, and anecdotal.

RECOMMENDATION SYSTEMS

Another concern is that recommendation algorithms may be creating radical 'filter bubbles'[11] amongst social media users. The former EU-Counter Terrorism Coordinator Gilles de Kerchove notes that the 'amplification of legal harmful content… may be conducive to radicalisation' (Council of the European Union 2020b, 7). In essence, the concern is that, broadly speaking, platforms have become considerably more adept at removing clearly illegal extremist content (such as group-branded material or beheading videos), but many malignant actors are deliberately skirting just below this threshold and creating 'borderline content' (as demonstrated by Conway, Watkin, and Looney 2022). Surveying 15 studies that empirically analyse recommendation systems and extremist content, Whittaker (2022b) suggests that this concern may be well-founded, finding that 10 did show that such material could be amplified. However, he also highlights several methodological limitations, such as a reliance on 'black box' studies that do not manipulate the platforms' algorithms; coding issues; and several studies that cannot account for user personalisation because of the way they access data. There is also a heavy emphasis in these studies towards English-language content and researching YouTube above other platforms (possibly due to its researcher-friendly API). One study not included in Whittaker's review was one carried out by Little and Richards (2021) which finds evidence of a 'rabbit hole' on TikTok between transphobic content on the platform and other right- wing extremist content. Similarly, analysing extremist content on the same platform, O'Connor (2021) finds that users were exploiting popular hashtags to game its recommendation algorithms in an attempt to reach as wide an audience as possible. Despite this well-founded concern, Whittaker (2022b) urges caution against the idea of 'radicalisation by algorithm,' arguing that we know little about user agency within this process and that the relationship between engaging with extreme content and become radicalised is a complex one.

COVID-19 RELATED ONLINE RADICALISATION

As outlined in Section 1, policymakers have expressed grave concerns that the COVID-19 pandemic and ensuing lockdowns may have created the 'perfect storm' of radicalisation, with millions of

[11] A 'filter bubble,' as coined by Eli Pariser in his 2011 book, *The Filter Bubble: What the Internet is Hiding from You*, is the concern that an increasing use of personalisation algorithms (such as recommendation systems, news results, and timelines) will amplify views that users already hold, while preventing them from coming into contact with new or dissenting ideas.

people spending countless hours in front of computer screens unsupervised, which may add to a range of grievances and stressors that people were experiencing. It should be underscored that two years into the pandemic is far too soon to make firm judgements about the long-term effects, however, we have started to see studies that can give some indication.

To begin with radicalisation more broadly, there is good reason to think that the material conditions brought about by the pandemic may include exacerbating factors. Marone (2021) outlines a range of factors that the academic literature suggest may be problematic, including loss and trauma; psychological distress; and high levels of uncertainty. Ackerman and Peterson (2020) also point to a range of factors that are congruent with the radicalisation literature: dislocation from daily lives, the loss of loved ones, loss of jobs, and uncertainty about the future. These factors could, they argue, lead to individuals being susceptible to extremist messaging which blames out-groups for their crises. Salman and Gill (2020) highlight a range of stressors that could increase vulnerability, such as isolation or mental health issues; economic factors (like those outlined above); or disruption in careers or education. These factors may coincide with more exposure to radical environments online which could lead to more support for violent extremism. This view is taken by Malik (2020) who argues that people would make sense of the crisis by engaging with fake news, conspiracy theories, and extremist materials online, which may exacerbate radicalisation.

It is also clear that extremist groups and movements have attempted to exploit the crisis by adapting their propaganda narratives to incorporate the pandemic. Jihadist groups such as IS were vocal and used it as an opportunity to call for attacks, while al-Qaeda (AQ) framed it as an opportunity to recruit new members – both groups gloated and said that it was divine retribution (al-Lami 2020). Europol (2021b) outlined three main narratives from jihadist groups: i) the negative impact on Western societies; ii) blaming Governments for the pandemic and framing a return to Islam as the solution and; iii) providing health and hygiene guidance to their supporters to demonstrate governance capabilities. Research has demonstrated that right-wing extremists adopted a similar approach; for example, conspiratorial COVID-19 narratives were present in French and German online ecosystems (Macdonald et al. 2022). Studies on Telegram also show the prevalence of such narratives; Gallagher and O'Connor (2021) and Schulze et al. (2022) both find that right-wing extremist conspiracy theories were rife on the platform in Irish and German groups respectively. Two reports into online activity in the US (Moonshot 2020b) and Canada (Moonshot 2020a) both found evidence to suggest that searches for white supremacist keywords increased after lockdowns were introduced. Similarly, Davies, Wu, and Frank (2021) found that traffic on right-wing extremist and involuntary celibate (Incel) forums showed a demonstrable increase in posting behaviours.

There are also some case studies of violent extremist plots that may suggest that COVID-19 grievances are important. Conway, Watkin, and Looney (2022) discuss the case of Jürgen Conings who was arrested in 2021 for attempted murder and illegal possession of weapons because he was alleged to be involved in threats to kill Marc Van Ranst, a Belgian virologist. They also point to the case of 'Mario N' who is accused of murdering a 20-year-old petrol station employee who refused him service for not wearing a mask. The alleged killer was active within the right-wing extremist online ecosystem and had expressed a rejection of lockdown policies. The family of the man accused of the attacks in Buffalo, NY, have also highlighted COVID-19 as a key factor, stating that the paranoia surrounding the virus, combined with the fact that he was spending all day on the Internet in isolation, could have exacerbated his radicalisation (Sarkar 2022).

Despite these well-founded concerns and case studies, there is good reason to be cautious of the idea of 'COVID-19 online radicalisation.' As this report has demonstrated in detail, the relationship between acting within radical networks online or engaging with propaganda and committing acts of violent extremism is an extremely complex one. Studies have repeatedly shown that offline interactions still remain a key part of radicalisation (Herath and Whittaker 2021; Whittaker 2021; Gill et al. 2017; Reynolds and Hafez 2019) and there is still much to learn about the relationship between consuming radical content and engaging in violence (Conway 2017; Wolfowicz, Hasisi, and Weisburd 2022).

The tentative early data do not support the idea that COVID-19 has increased the threat of violent extremism. Despite some case studies appearing, such as those outlined above, quantitative research suggests that attacks may be at a stable – or even declining – rate. Europol's Terrorism Situation and Trend reports provide key indicators here; for example, the 2021 version found that terrorist attacks remained stable between 2019 and 2020, while there was a sharp drop in arrests (Europol 2021a). Moreover, the 2022 report saw the number of attacks and arrests fall yet again (Europol 2022). King and Mullins (2021) offer an early snapshot, finding that jihadist attacks in the West in 2020 were roughly in line with the average since 2014. They report that the number of violent right-wing extremist attacks did increase, but again did so at a rate that is congruent with the previous years. Pantucci (2021) drew from six different databases for the year 2020, demonstrating that attacks in Europe increased, though globally, violence is down. On the other hand, Berman et al. (2022) use data from 2016-2020 to assess the effects of lockdown policies, finding there to be a sharp decrease in demonstrations in the first few months after they were introduced, though numbers quickly rose back to their normal levels. They find that in countries that have risk factors for conflict (such as poverty; authoritarianism; and high levels of polarisation) violence actually intensifies. The picture will become clearer as the years progress, but each of these pieces of research are reticent to ascribe a causal link between a single factor, such as the pandemic, let alone the increased time spent online as a result of it, to a rise in violent extremism. Rather, radicalisation is a complex process which includes factors on the personal, environmental, and systemic level (Bouhana 2019).

THINKING ABOUT THE FUTURE

Thus far, this section has considered the contemporary picture of online radicalisation. Before finishing, it is worthwhile to contemplate how this situation may develop in the future. This should not be taken as a prediction; research in this field, and in the social sciences more broadly, is littered with surprising turns and bold conjecture that did not come to pass. Rather, this section is intended as food for thought for the ways in which online radicalisation may change in the coming years.

The most anticipated and well-publicised online technological advancement is the move towards the 'metaverse.' In 2021, Facebook rebranded itself as Meta and announced that it would focus heavily on the upcoming 'metaverse,' which they stated would be 'the next evolution in social connection and the successor to the mobile Internet… [which will] help you connect with people when you aren't physically in the same place and get us even closer to that feeling of being together in person' (Meta 2022). Although it is unclear exactly what it will entail, the 'metaverse' will include aspects of virtual and augmented reality and operate as a space for gaming, socialising, and e-commerce (Ravenscraft 2022). Lakhani, White, and Wallner (2022) note that, like any emerging technology, the 'metaverse' will bring emerging risks from violent extremist actors. In particular, they are concerned with the overlap with 'gamification,' particularly game-adjacent platforms such as 8chan and 8kun, which are home to large amounts of radical content. Elson, Doctor, and Hunter (2022) highlight three ways in which the 'metaverse' may be exploited by extremists: recruitment, coordination, and target selection. The first of these is particularly relevant with regard to online radicalisation. They note that a resurrected bin Laden could speak to followers in a virtual rose garden or lecture hall, allowing new leaders to build and maintain extreme ideological and social communities.

The sub-section on online environments demonstrates that extremists will innovate when faced with a hostile ecosystem. It shows that they had the freedom to post on a wide range of platforms with relatively little content moderation in the mid-2010s and, when that became impossible, they developed more sophisticated systems to maintain an online presence (for example, see Fisher, Prucha, and Winterbotham 2019). This will continue to be the case as policy manoeuvres continue to focus on content removal. Gartenstein-Ross, Clarke, and Shear (2020) offer a four-step model to understand how violent extremists innovate. They begin with *Early Adoption* before technologies undergo consumer-focused improvements. The next phase is *Iteration*, which leads to the third step, a *Breakthrough,* in which extremists begin to find regular success. Finally, there is a period of *Competition* in which both extremists and societal stakeholders go through a cycle of adaption and

counter-adaption. They frame this in the context of social media usage, showing how jihadists first used these platforms, before eventually finding success and being countered with content removal, before then moving to more security-focused platforms.

This should be a concern to policymakers given that research has suggested that moving terrorists away from larger platforms to ones that offer greater operational security and do not comply with court orders (such as Telegram), may hamper law enforcement's ability to conduct investigations (Whittaker 2021; Jensen et al. 2018). The discussion above of the adoption of the decentralised web can be seen within this framework, too. Extremist supporters found it difficult to maintain a presence on mainstream platforms so instead adopted more innovative measures. Hamid and Ariza (2022) argue that it is vital to consider technological developments as the landscape moves so quickly and existing policies are often reactive. In essence, the pace of online technologies can be measured in hours, while it often takes years to introduce regulation.

Part of the breakneck pace of technological innovation is the enmeshing of the online and offline domains, which will likely render the notion of 'online radicalisation' redundant. Internet philosophers have dubbed this state as 'Onlife' (Floridi 2015). We no longer 'go online' – this is a relic of the 1990s in which individuals had to make a deliberate decision to dial up a modem and sit in front of a PC. Now our smart devices and mobile data mean that we are almost always online, and even when we are not, social media affects our offline activity, and vice versa – how we act online affects what we see online (Jurgenson 2012). This has important ramifications when it comes to online radicalisation, with Valentini, Lorusso, and Stephan (2020) arguing that online and offline radical milieus are not easily demarcated but conflate in unprecedented ways and integrate elements that pertain to both. Whittaker (2022c) develops this argument by highlighting behaviours which demonstrate this, such as individuals engaging in 'viewing parties' by congregating at one member's house and watching propaganda together and discussing it afterwards, often exchanging tablets or smart phones between one other with recommendations for further watching. This new state of 'onlife' is largely a result of new technologies blurring the two domains and as we hurtle towards the 'metaverse,' the Web 3.0, and a greater emphasis on virtual/augmented reality, this distinction will become even less pronounced.

CONCLUSION

This report has provided an overview of the current state of knowledge of online radicalisation. To do so, it first outlined how it has been framed by policymakers, the press, and academics. Importantly, while policymakers and journalists have repeatedly highlighted radicalisation via the Internet as a concern, researchers have instead attempted to bring nuance into the debate by suggesting that it is conceptually unclear and that there is still much to learn about the role that the Internet plays in this process. The second section sets out a brief history of online radicalisation, showing how we got to this point. While the concept emerged in the mid-2000s, research into terrorists' use of the Internet goes back over twenty years, which is roughly when the first known extremist websites and forums appeared. The section also outlines the growth of online jihadist and violent right-wing extremist movements throughout the 2010s, highlighting key players such as the radical cleric Anwar al-Awlaki and Atomwaffen Division.

Having tackled how the issue is framed and its history, the bulk of the report focuses on the contemporary picture of online radicalisation. One of the best ways to take stock of this is by conducting literature and systematic reviews. By and large, these studies point to radicalisation as a complex social phenomenon with many factors involved. While certain types of online activity may be a risk factor, it is one of many in a process that is ill-understood. Several reviews also point to the lack of rich data when studying the topic. Studies that have created and analysed databases of terrorists have often downplayed the idea of online radicalisation, instead showing that

behaviours tend to be split over both domains and that offline interactions are still key. Of the few studies that have drawn from an experimental design in recent years, there is good reason to think that the consumption of radical propaganda may be persuasive in its target audience, but only if those exposed have a specific personality trait or engage in subversive online behaviour. The report then pivots to review the contemporary ecosystem that a radicalising individual may find online. Neither jihadists nor violent right-wing extremists currently enjoy the freedom on mainstream social media platforms that they once did, but instead are using a host of end-to-end encrypted, decentralised, or alt-tech platforms. If they wish to remain on mainstream platforms, they have had to adapt their posting behaviours to avoid content removal. It also discusses other contemporary issues, such as the use of websites, gaming technologies, and recommendation systems. The section ends by reflecting on the past two ''COVID-19-era' years, questioning whether the host of risk factors, combined with the countless extra hours spent online pose a threat.

Considering everything presented in this report, it becomes apparent that online radicalisation is a complex phenomenon with many equivocations. Terrorists may be using the Internet more than ever before, but offline interactions remain key. Propaganda is shown to be persuasive, but under a specific set of circumstances. Extremists are adopting online gaming spaces, but there is little-to-no evidence that groups are using them for direct recruitment. Recommendation systems may promote radical content, but it is likely that users' own choices play a larger role than that of algorithms. Although the exploitation of the Internet clearly poses a risk from a security perspective, it is vital that the concern remains in perspective and policy responses do not come at the expense of offline interventions, such as capacity and resilience building, safeguarding programmes, and digital literacy. Rather than a specific policy focus on online radicalisation, decision-makers should consider a multi-level approach which includes an individual's personal susceptibility; how likely they are (by both their own choices and where they are located) to be exposed to radicalising influences; whether their environment is likely to act as an exacerbator or protective factor; as well as systemic level factors (Bouhana 2019). Online activity can impact many of these levels but is not necessarily the driving force behind any of them. In essence, people should focus more on the 'radicalisation' and put less emphasis (though by no means none) on the online domain. It is a piece of the puzzle, but only one.

This report has also highlighted where there are some key gaps in the literature. To begin with the previous point, existing online radicalisation research fixates heavily on whether certain behaviours take place online or offline and try to judge whether one is more (or less) important. There has been little literature which attempts to understand how communications technologies interplay with the wider environment (across both domains) and affect an individual's propensity to engage in violent extremism (Whittaker 2022a). Across the board, scholars are concerned with the lack of rich data to better understand the problem. Secondly, studies that use an experimental design to understand the effects of propaganda are increasing but are still rare. As more of these studies emerge, they will likely run into the same problem as other fields of research which delve into the effects of violent media – it is relatively easy to establish whether individuals are affected in the short term, but they cannot take into account the complex social process of daily life and interactions with peers (Braddock 2022). If the policymakers' concern is *prolonged* exposure to extremist content, then scholars will have to find a way of creating longitudinal designs, but this is likely to be problematic for ethical reasons.

Thirdly, as highlighted in the section on covid 19, much of the concern around online radicalisation relates to the quantity of time spent online and much of the data that is available discusses the lengths of time in which people are using the Internet. However, much less is known about the importance of the *quality* of time spent online. For example, if an individual is completely immersed within an extremist online network with no dissenting voices, it stands to reason that it is likely to be a greater risk factor than someone who spends more time online, but engages with content in a more passive manner. A final methodological gap is base rates; there is very little understanding of the societal prevalence of most online radicalisation indicators (Gill 2016). While some studies have begun to answer this question (for example, see: Clemmow et al. 2020; Rottweiler and Gill 2020),

if we do not know how often the non-radicalised population is engaging in certain behaviours, then we cannot know if it is a risk factor.

ABOUT THE AUTHOR

Joe Whittaker is a lecturer in Cyber Threats at Swansea University in the Department of Criminology, Sociology, and Social Policy. He is primarily interested in online radicalisation, which encapsulates behavioural studies of terrorists' use of the Internet; experiments into the role of recommendation algorithms; and researching extremist groups' use of video games. He also researches and teaches on how stakeholders respond, particularly in terms of counter-narratives, digital literacy, and regulation. He regularly presents his research to academic, policymaker, and practitioner audiences.

REFERENCES

Ackerman, Gary, and Hayley Peterson. 2020. "Terrorism and COVID-19: Actual and Potential Impacts." *Perspectives on Terrorism* 14 (3): 59–73.

Aly, Anne. 2017. "Brothers, Believers, Brave Mujahideen: Focusing Attention on the Audience of Violent Jihadist Preachers." *Studies in Conflict & Terrorism* 40 (1): 62–76. https://doi.org/10.1080/1057610X.2016.1157407.

Amarasingam, Amarnath, Marc-André Argentino, and Graham Macklin. 2022. "The Buffalo Attack: The Cumulative Momentum of Far-Right Terror." *CTC Sentinel*, July: 1–10.

Arquilla, John, Ronfeldt, David, and Zanini, Michele. 1999. "Networks, Netwar, and Information-Age Terrorism," in: Lesser et al. [Eds.] *Countering the New Terrorism*, RAND Corporation.

Back, Les. 2002. "Aryans Reading Adorno: Cyber-Culture and Twenty-First-Century Racism." *Ethnic and Racial Studies* 25 (4): 628–51. https://doi.org/10.1080/01419870220136664.

Baele, Stephane J., Lewys Brace, and Travis G. Coan. 2020. "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda." *Studies in Conflict and Terrorism*.

Bartlett, Jamie. 2015. *The Dark Net*. London: Windmill Books.

Bastug, Mehmet F, Aziz Douai, and Davut Akca. 2018. "Exploring the 'Demand Side' of Online Radicalization: Evidence from the Canadian Context." *Studies in Conflict & Terrorism*.

Behr, Ines von, Anais Reding, Charlie Edwards, and Luke Gribbon. 2013. "Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism." *RAND* Corporation.

Benson, David C. 2014. "Why the Internet Is Not Increasing Terrorism." *Security Studies* 23 (2): 293–328.

Bermingham, Adam, Conway, Maura, McInerney, Lisa, O'Hare, Neil, and Smeaton, Alan F. 2009. "Combining social network analysis and sentiment analysis to explore the potential for online radicalisation" Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining, ASONAM 2009 : 231-236.

Berger, J.M., and Jonathon 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* March (20).

Berger, J.M., and Heather Perez. 2016. "The Islamic State's Diminishing Returns on Twitter: How Suspensions Are Limiting the Social Networks of English-Speaking ISIS Supporters." *George Washington University: Program on Extremism*.

Berman, Nicholas, Mathieu Couttenier, Nathalie Monnet, and Rohit Ticku. 2022. "Shutdown Policies and Conflict Worldwide." *Journal of Comparative Economics* 50: 240–55.

Bloom, Mia, Hicham Tiflati, and John Horgan. 2017. "Navigating ISIS's Preferred Platform: Telegram." *Terrorism and Political Violence*, 1–13. https://doi.org/10.1080/09546553.2017.1339695.

Borum, Randy. 2011. "Rethinking Radicalization." *Journal of Strategic Security* 4 (4): 1–6.

Bouhana, Noémie. 2019. "The Moral Ecology of Extremism: A Systemic Perspective." *Commission for Countering Extremism*.

Braddock, Kurt. 2022. "Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda." *Terrorism and Political Violence* 34 (2): 240–62.

Braddock, Kurt, Brian Hughes, Beth Goldberg, and Cynthia Miller-Idriss. 2022. "Engagement in Subversive Online Activity Predicts Susceptibility to Persuasion by Far-Right Extremist Propaganda." *New Media & Society*.

Braddock, Kurt, Sandy Schumann, Emily Corner, and Paul Gill. 2022. "The Moderating Effects of 'Dark' Personality Traits and Message Vividness on the Persuasiveness of Terrorist Narrative Propaganda." *Frontiers in Psychology* 13 (July).

Carter, Joseph, Shiraz Maher, and Peter Neumann. 2014. "#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks." *The International Centre for the Study of Radicalisation and Political Violence*.

Clemmow, Caitlin, Sandy Schumann, Nadine L Salman, and Paul Gill. 2020. "The Base Rate Study: Developing Base Rates for Risk Factors and Indicators for Engagement in Violent Extremism." *Journal of Forensic Sciences*.

Clifford, Bennett, and Helen Powell. 2019. "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." *Program on Extremism*, no. June.

Cohen-Almagor, Raphael. 2014. "Countering Hate on the Internet." *Annual Review of Law and Ethics* 22: 431–43.

Conway, Maura. 2002. "Reality Bytes: Cyberterrorism and Terrorist 'use' of the Internet." *First Monday* 7 (11): 1–17.

Conway, M. 2006. "Terrorism and the Internet: New Media–New Threat?" *Parliamentary Affairs* 59(2), 283–298.

Conway, Maura. 2016. "Violent Extremism and Terrorism Online in 2016: The Year in Review." *Vox Pol*.

Conway, Maura. 2017. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism* 40 (1): 77–98.

Conway, Maura. 2020. "Routing the Extreme Right: Challenges for Social Media Platforms." *RUSI Journal* 165 (1): 108–13.

Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weir. 2018. "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." *Studies in Conflict and Terrorism* 42 (1–2): 141–60.

Conway, Maura, and Seán Looney. 2022. "Back to the Future? Twenty First Century Extremist and Terrorist Websites." *Radicalisation Awareness Network*.

Conway, Maura, Amy-Louise Watkin, and Seán Looney. 2022. "Violent Extremism and Terrorism Online in 2021: The Year in Review." *Radicalisation Awareness Network*.

Cook, Joana, and Gina Vale. 2019. "From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of

the Caliphate." *International Centre for the Study of Radicalisation*.

Corner, Emily, Paul Gill, and Oliver Mason. 2016. "Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence" *Studies in Conflict & Terrorism*, 39(6); 560-568.

Cottee, Simon. 2020. "Incel (E)Motives: Resentment, Shame and Revenge." *Studies in Conflict and Terrorism* 44 (2): 93–114. https://doi.org/10.1080/1057610X.2020.1822589.

Council of Europe. 2014. "Revised EU Strategy for Combatting Radicalisation and Recruitment to Terrorism." 9956/14.

Council of the European Union. 2020a. "Online Gaming in the Context of the Fight against Terrorism." https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf.

Council of the European Union. 2020b. "The Role of Algorithmic Amplification in Promoting Violent and Extremist Content and Its Dissemination on Platforms and Social Media." Vol. December 2.

Datareportal. 2022. "Digital Around the World." https://datareportal.com/global-digital-overview.

Dauber, Cori E, Mark D Robinson, Jovan J Baslious, and Austin G Blair. 2019. "Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos." *Perspectives on Terrorism* 13 (3): 17–31.

Davey, Jacob. 2021. "Gamers Who Hate: An Introduction to ISD's Gaming and Extremism Series." *Institute for Strategic Dialogue*. https://www.isdglobal.org/isd-publications/gamers-who-hate-an-introduction-to-isds-gaming-and-extremism-series/.

Davies, Garth, Edith Wu, and Richard Frank. 2021. "A Witch's Brew of Grievances: The Potential Effects of COVID-19 on Radicalization to Violent Extremism." *Studies in Conflict and Terrorism*.

Ducol, Benjamin. 2015. "A Radical Sociability: In Defense of an Online/Offline Multidimensional Approach to Radicalization." In *Social Networks, Terrorism, and Counter-Terrorism: Radical and Connected*, edited by Martin Bouchard, 82–104. London: Routledge.

Elson, Joel. S, Doctor, Austin, C., and Hunter, Sam. 2022. The Metaverse Offers a Future Full of Potential – For Terrorists and Extremists, Too. *Vox Pol Blog*, https://www.voxpol.eu/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too/.

European Commission. 2015. "The European Agenda on Security". Com. 185.

European Commission. 2020. "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond."

European Commission. 2022. "Digital Economy and Society Index."

Europol. 2020. "European Union Terrorism Situation and Trend Report."

Europol. 2021a. "European Union Terrorism Situation and Trend Report".

Europol. 2021b. "Online Jihadist Propaganda."

Europol. 2022. "Terrorism Situation and Trend Report: 2022."

Federal Bureau of Investigation, nd, "What We Investigate – Terrorism," https://www.fbi.gov/investigate/terrorism.

Fisher, Ali, Nico Prucha, and Emily Winterbotham. 2019. "Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability." *Global Research Network on Terrorism and Technology*, no. 6.

Floridi, Luciano. 2015. "Designing the Public Sphere: Information Technologies and the Politics of Mediation." In *The Onlife Manifesto: Being Human in a Hyperconnected Era*, edited by Luciano Floridi, 7–17. SpringerOpen.

Gallagher, Aoife, and Ciarán O'Connor. 2021. "Layers of Lies: A First Look at Irish Far-Right Activity on Telegram." *Institute for Strategic Dialogue*.

Gallagher, Aoife, Ciaran O'Connor, Pierre Vaux, Elise Thomas, and Jacob Davey. 2021. "The Extreme Right on Discord." *Institute for Strategic Dialogue*.

Gill, Paul. 2016. "Online Behaviours of Convicted Terrorists." *Vox Pol*.

Gill, Paul, and Emily Corner. 2015. "Lone Actor Terrorist Use of the Internet and Behavioural Correlates." In *Terrorism Online: Politics Law and Technology*, edited by Lee Jarvis, Stuart Macdonald, and Thomas M. Chen, 35–53. Abingdon, Oxon: Routledge.

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes." *Criminology and Public Policy* 16 (1): 99–117.

Gill, Paul, Emily Corner, A Thornton, and Maura Conway. 2015. "What Are the Roles of the Internet in Terrorism?" *Vox Pol*.

Glazzard, Andrew. 2019. "Shooting the Messenger: Do Not Blame the Internet for Terrorism." *RUSI Newsbrief* 39 (1).

Gough, Sarah. 2021. "Caleb Cain: Former far-right extremist says 'no one has a strategy' for ongoing threat" *Sky News*, 25 Febuary. https://news.sky.com/story/caleb-cain-former-far-right-extremist-says-no-one-has-a-strategy-for-ongoing-threat-12228120.

Grinnell, Daniel, Stuart Macdonald, and David Mair. 2017. "The Response of, and on, Twitter to the Release of Dabiq Issue 15." *Europol Public Information*.

Grinnell, Daniel, Stuart Macdonald, David Mair, and Nuria Lorenzo-Dus. 2018. "Who Disseminates Rumiyah? Examining the Relative Influence of Sympathiser and Non-Sympathiser Twitter Users."

Hafez, Mohammed M., and Creighton Mullins. 2015. "The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism." *Studies in Conflict & Terrorism* 38 (11): 958–75.

Hamid, Nafees, and Cristina Ariza. 2022. "Offline Versus Online Radicalisation: Which Is the Bigger Threat?" *Global Network on Extremism & Technology*.

Hassan, Ghayda, Sébastien Brouillette-Alarie, Séraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnpaul Varela, et al. 2018. "Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence." *International Journal of Developmental Sciences* 12 (1–2): 71–88.

Herath, Chamin, and Joe Whittaker. 2021. "Online Radicalisation: Moving beyond a Simple Dichotomy." *Terrorism and Political Violence*.

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

Hoffman, Bruce, Jacob Ware, and Ezra Shapiro. 2020. "Assessing the Threat of Incel Violence." *Studies in Conflict and Terrorism* 43 (7): 565–87.

Horgan, John. 2008. "From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism." *The Annals of the American Academy of Political and Social Science* 618 (1): 80–94.

Hurst, Daniel. 2022. "Asio boss warns of 'angry and isolated' Australians radicalised during pandemic," *The Independent*, 9 February. https://www.theguardian.com/australia-news/2022/feb/09/violent-extremists-asio-boss-warns-of-angry-and-isolated-australians-radicalised-during-pandemic.

Jensen, Michael, Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, and Elizabeth Yates. 2018. "The Use of Social Media by United States Extremists." *National Consortium for the Study of Terrorism and Responses to Terrorism*.

http://www.start.umd.edu/data-.

Jurgenson, Nathan. 2012. “When Atoms Meet Bits: Social Media, the Mobile Web and Augmented Revolution.” *Future Internet* 4 (1): 83–91. https://doi.org/10.3390/fi4010083.

Kenyon, Jonathan, Jens Binder, and Christopher 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 & Terrorism*. https://doi.org/10.1080/1057610X.2022.2065902.

Ki-moon, B. 2016. More ‘Concrete Steps’ Needed by Nations to Counter Terrorism, Ban Tells Security Council, *UN News*. https://news.un.org/en/story/2016/04/526712-more-concrete-steps-neededнations-counter-terrorism-ban-tells-security-council.

King, Michael and Mullins, Sam. 2021. “COVID-19 and Terrorism in the West: Has Radicalization Really Gone Viral?” *Just Security*, https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral/.

Klausen, Jytte. 2015. “Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq.” *Studies in Conflict & Terrorism* 38 (1): 1–22.

Koehler, Daniel, Verena Fiebig, and Irina Jugl. 2022. “From Gaming to Hating: Extreme - Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms.” *Political Psychology*. https://doi.org/10.1111/pops.12855.

Lakhani, Suraj. 2022. “Video Gaming and (Violent) Extremism: An Exploration of the Current Landscape, Trends, and Threats.” *Radicalisation Awareness Network*.

Lakhani, Suraj, and Susann Wiedlitzka. 2022. ““Press F to Pay Respects": An Empirical Exploration of the Mechanics of Gamification in Relation to the Christchurch Attack.” *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2022.2064746.

Lakomy, Miron. 2017a. “Cracks in the Online ‘Caliphate’: How the Islamic State Is Losing Ground in the Battle for Cyberspace.” *Perspectives on Terrorism* 11 (3): 40–53.

Lakomy, Miron. 2017b. “Let’s Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment.” *Studies in Conflict & Terrorism*.

Al-Lami, Mina. 2020. “Jihadists see COVID-19 as an Opportunity”, *Global Network on Extremism & Technology*, https://gnet-research.org/2020/06/01/jihadists-see-covid-19-as-an-opportunity/.

Lamphere-Englund, Galen and White, Jessica. 2022. “The Buffalo Attack and the Gamification of Violence” *Royal United Services Institute*.

Levin, B. 2015. “The Original Web of Hate: Revolution Muslim and American Homegrown Extremists.” *American Behavioral Scientist* 59 (12): 1609–30.

Levin, Brian. 2002. “Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer Networks in America.” *American Behavioral Scientist* 45 (6): 958–88.

Little, Olivia and Richards, Abbie. 2021. “TikTok's algorithm leads users from transphobic videos to far-right rabbit holes” *Media Matters*.

Macdonald, Stuart, and Joe Whittaker. 2019. “Online Radicalization: Contested Terms and Conceptual Clarity.” In *Online Terrorist Propaganda, Recruitment, and Radicalisation*, 33–46. Boca Raton, FL: CRC Press.

Macdonald, Stuart, Kamil Yilmaz, Chamin Herath, J.M. Berger, Suraj Lakhani, Lella Nouri, and Maura Conway. 2022. “The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German & French Far-Right Ecosystems.” *Resolve Network*, May.

Malik, Nikita. 2020. "Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism" *Foreign Policy,* 26 March. https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/.

Marone, Francesco. 2021. "Hate in the Time of Coronavirus: Exploring the Impact of the COVID-19 Pandemic on Violent Extremism and Terrorism in the West." *Security Journal*.

Marwick, Alice, Benjamin Clancy, and Katherine Furl. 2022. "Far-Right Online Radicalization." *Center for Information, Technology, and Public Life*.

Meleagrou-Hitchens, Alexander. 2020. "*Incitement: Anwar Al-Awlaki's Western Jihad*." Cambridge, MA: Harvard University Press.

Meleagrou-Hitchens, Alexander, and Nick Kaderbhai. 2017. "Research Perspectives on Online Radicalisation: A Literature Review, 2006-2016." *Vox Pol*.

Meta. 2022. "What is the Metaverse?" https://about.meta.com/what-is-the-metaverse/.

Moonshot. 2020a. "The Impact of COVID-19 on Canadian Search Traffic," no. June. https://moonshotteam.com/covid-19-increase-in-searches-for-violent-far-right-content-in-canada/.

Moonshot. 2020b. "The Impact of Social Distancing on Engagement with Violent Extremist Content Online in the United States".

Neumann, Peter. 2013. "Options and Strategies for Countering Online Radicalization in the United States." *Studies in Conflict & Terrorism* 36 (6): 431–59.

Nouri, Lella, Nuria Lorenzo-Dus, and Amy-louise Watkin. 2019. "Following the Whack-a-Mole Britain First's Visual Strategy from Facebook to Gab." *Global Research Network on Terrorism and Technology*, no. 4.

O'Connor, Ciarán. 2021. "Hatescape : An In-Depth Analysis of Extremism and Hate Speech on TikTok." *Institute for Strategic Dialogue*, 57.

O'Rourke, Simon. 2007. "Virtual Radicalisation: Challenges for Police." *Proceedings of The 8th Australian Information Warfare and Security Conference*, 29–35.

Odağ, Özen, Anne Leiser, and Klaus Boehnke. 2020. "Reviewing the Role of the Internet in Radicalization Processes." *Journal for Deradicalization*, no. 21: 261–300.

Organization for Security and Co-operation in Europe. "Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach." 2013.

Pantucci, Raffaello. 2021. "Mapping the One-Year Impact of COVID-19 on Violent Extremism." *International Centre for Political Violence and Terrorism Research* 13 (2): 1–9.

Pauwels, Annelies. 2021. "Contemporary Manifestations of Violent Right-Wing Extremism in the EU: An Overview of P/CVE Practices." *Radicalisation Awareness Network*, 1–16.

Pearson, Elizabeth. 2016. "The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad" *Policy & Internet* 8(1): 5-33.

Post, Jerold, Cody McGinnis, and Kristen Moody. 2014. "The Changing Face of Terrorism in the 21st Century: The Communications Revolution and the Virtual Community of Hatred." *Behavioral Sciences & the Law* 32 (2): 306–36.

Prucha, Nico. 2016. "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram." *Perspectives on Terrorism* 10 (6): 48–58.

Radicalisation Awareness Network. 2021. "Preventing Radicalisation to Terrorism and Violent Extremism: Approaches and Practice" https://home-affairs.ec.europa.eu/system/files/2021-05/ran_collection-approaches_and_practices_en.pdf.

Ravenscraft, Eric. 2022. "What is the Metaverse, Exactly?" *Wired*, April 25. https://www.wired.com/story/what-is-the-metaverse/.

Reynolds, Sean C., and Mohammed M. Hafez. 2019. "Social Network Analysis of German Foreign Fighters in Syria and Iraq." *Terrorism and Political Violence* 31 (4): 661–86.

Robertson, David G., and Amarnath Amarasingam. 2022. "How Conspiracy Theorists Argue: Epistemic Capital in the QAnon Social Media Sphere." *Popular Communication* 00 (00): 1–15.

Robinson, Nick, and Joe Whittaker. 2021. "Playing for Hate? Extremism, Terrorism, and Videogames." *Studies in Conflict & Terrorism*.

Rodriguez, Salvador. 2021. 'QAnon and anti-vaxxers brainwashed kids stuck at home — now teachers have to deprogram them,' *CNBC*, 7 September, https://www.cnbc.com/2021/09/04/qanon-and-anti-vaxxers-brainwashed-kids-stuck-at-home-during-pandemic.html.

Rottweiler, Bettina, and Paul Gill. 2020. "Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-Efficacy, Self-Control and Law-Related Morality." *Terrorism and Political Violence*.

Rutte, M. 2017, "Short Speech by Prime Minister Mark Rutte for the Side Event on Online Radicalisation." Government of the Netherlands.

Ryan, Johnny. 2007. "*Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web*." Dublin: Institute of European Affairs.

Sageman, Marc. 2004. "*Understanding Terror Networks*." Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. 2008. "The Next Generation of Terror." *Foreign Policy*, March/April: 36–42.

Sageman, M. 2014. "The Stagnation in Terrorism Research." *Terrorism and Political Violence* 26 (4): 565–80. https://doi.org/10.1080/09546553.2014.895649.

Salman, Nadine L, and Paul Gill. 2020. "Terrorism during the COVID-19 Pandemic." *University College London*, no. 13.

Sarkar, Alisha. 2022. "Buffalo shooting: Payton Gendron's family blame Covid isolation" *The Independent*, 17 May. https://www.independent.co.uk/news/world/americas/crime/buffalo-shooting-payton-gendron-covid-b2080541.html.

Schlegel, Linda. 2020. "Jumanji Extremism? How Games and Gamification Could Facilitate Radicalization Processes." *Journal for Deradicalization*, no. 23: 1–44.

Schlegel. 2021. "The Role of Gamification in Radicalization Processes." *Modus/Zad Working Paper*.

Schulze, Heidi, Julian Hohner, Simon Greipl, Maximilian Girgnhuber, Isabell Desta, and Diana Rieger. 2022. "Far-Right Conspiracy Groups on Fringe Platforms: A Longitudinal Analysis of Radicalization Dynamics on Telegram." *Convergence: The International Journal of Research into New Media Technologies*.

Schuurman, Bart, and Max Taylor. 2018. "Reconsidering Radicalization: Fanaticism and the Link Between Ideas and Violence." *Perspectives on Terrorism* 12 (1): 3–22.

Scrivens, Ryan, Tiana Gaudette, Maura Conway, and Thomas J Holt. 2022. "Right-Wing Extremists' Use of the Internet: Emerging Trends in the Empirical Literature." In *Right-Wing Extremism in Canada and the United States*, edited by Barbara Parry, Jeff Gruenewald, and Ryan Scrivens, 355–80. Palgrave Hate Studies.

Sedgwick, Mark. 2010. "The Concept of Radicalization as a Source of Confusion." *Terrorism and Political Violence* 22 (4): 479–94. https://doi.org/10.1080/09546553.2010.491009.

Selepak, Andrew. 2010. "Skinhead Super Mario Brothers: An Examination of Racist and Violent Games on White Supremacist

Web Sites." *Journal of Criminal Justice and Popular Culture* 17 (1): 1–47.

Tait, Amelia. 2017. "We Need to Talk about the Online Radicalisation of Young, White Women, *New Statesman*, 18 August. https://www.newstatesman.com/long-reads/2017/08/we-need-talk-about-online-radicalisation-young-white-women.

Tech Against Terrorism. 2021a. "Terrorist Content Analytics Platform: Transparency Report."

Tech Against Terrorism. 2021b. "Trends in Terrorist and Violent Extremist Use of the Internet | Q1-Q2 2021."

Tech Against Terrorism. 2022. "The Threat of Terrorist and Violent Extremist-Operated Websites."

Thorleifsson, Cathrine, and Joey Duker. 2021. "Lone Actors in Digital Environments." *Radicalisation Awareness Network*.

Tufekci, Zeynep. 2018. "YouTube, the Great Radicalizer," *New York Times*, March 10, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politicsradical.html.

UN CTED. 2015. "Analysis and Recommendations with Regard to the Global Threat from Foreign Fighters."

UN CTED. 2020. "The Impact of the Covid-19 Pandemic on Terrorism, Counter-Terrorism and Countering Violent Extremism."

United Nations Security Council. 2014. Resolution 2187 (S/Res/2178).

Valentini, Daniele, Anna Maria Lorusso, and Achim Stephan. 2020. "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization." *Frontiers in Psychology* 11 (March).

Ware, Jacob. 2020. "Fighting Back: The Atomwaffen Division, Countering Violent Extremism, and the Evolving Crackdown on Far-Right Terrorism in America." *Journal for Deradicalization*, no. 25: 74–116.

Washington Post Editorial Board. 2019. "Beware the Rabbit Hole of Radicalization," August 6. https://www.washingtonpost.com/opinions/beware-the-rabbit-hole-of-radicalization/2019/08/06/0d589a96-b7bc-11e9-a091-6a96e67d9cce_story.html.

Weimann, Gabriel. 2004. "Www.Terror.Net - How Modern Terrorism Uses the Internet." *USIP Special Report*, 1–12.

Weimann. 2012. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3 (2): 75–90.

Whittaker, Joe. 2020. "Online Echo Chambers and Violent Extremism." In *The Digital Age, Cyber Space, and Social Media: The Challenges of Security & Radicalization*, edited by Syed Munir Khasru and Riasat Noor, 129–50. Dhaka: Institute for Policy, Advocacy, and Governance.

Whittaker, Joe. 2021. "The Online Behaviors of Islamic State Terrorists in the United States." *Criminology and Public Policy* 20: 177–203. https://doi.org/10.1111/1745-9133.12537.

Whittaker, Joe. 2022a. "Online Radicalisation: The Use of the Internet by Islamic State Terrorists in the US (2012-2018)." Doctoral Thesis. Swansea University & Leiden University.

Whittaker, Joe. 2022b. "Recommendation Algorithms and Extremist Content: A Review of Empirical Evidence." *Global Internet Forum to Counter-Terrorism*.

Whittaker, Joe. 2022c. "Rethinking Online Radicalization." *Perspectives on Terrorism* 16 (4): 27–40.

Wiktorowicz, Q., 2013. "Working to Counter Online Radicalization to Violence in the United States," White House Blog. https://obamawhitehouse.archives.gov/blog/2013/02/05/working-counteronline-radicalization-violence-united-states.

Winter, Charlie, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino, and Johanna Fürst. 2020. "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies." *International Journal of Conflict and Violence* 14 (2): 1–20.

Wolfowicz, Michael, Badi Hasisi, and David Weisburd. 2022. "What Are the Effects of Different Elements of Media on Radicalization Outcomes? A Systematic Review." *Campbell Systematic Reviews* 18 (2).

Wood, Poppy. 2021. 'Lone wolf' terrorists who have 'self-radicalised' online during Covid pandemic becoming an increasing concern, *I Newspaper*, 16 November. https://inews.co.uk/news/lone-wolf-terrorists-self-radicalised-online-during-covid-pandemic-increasing-concern-1304430.