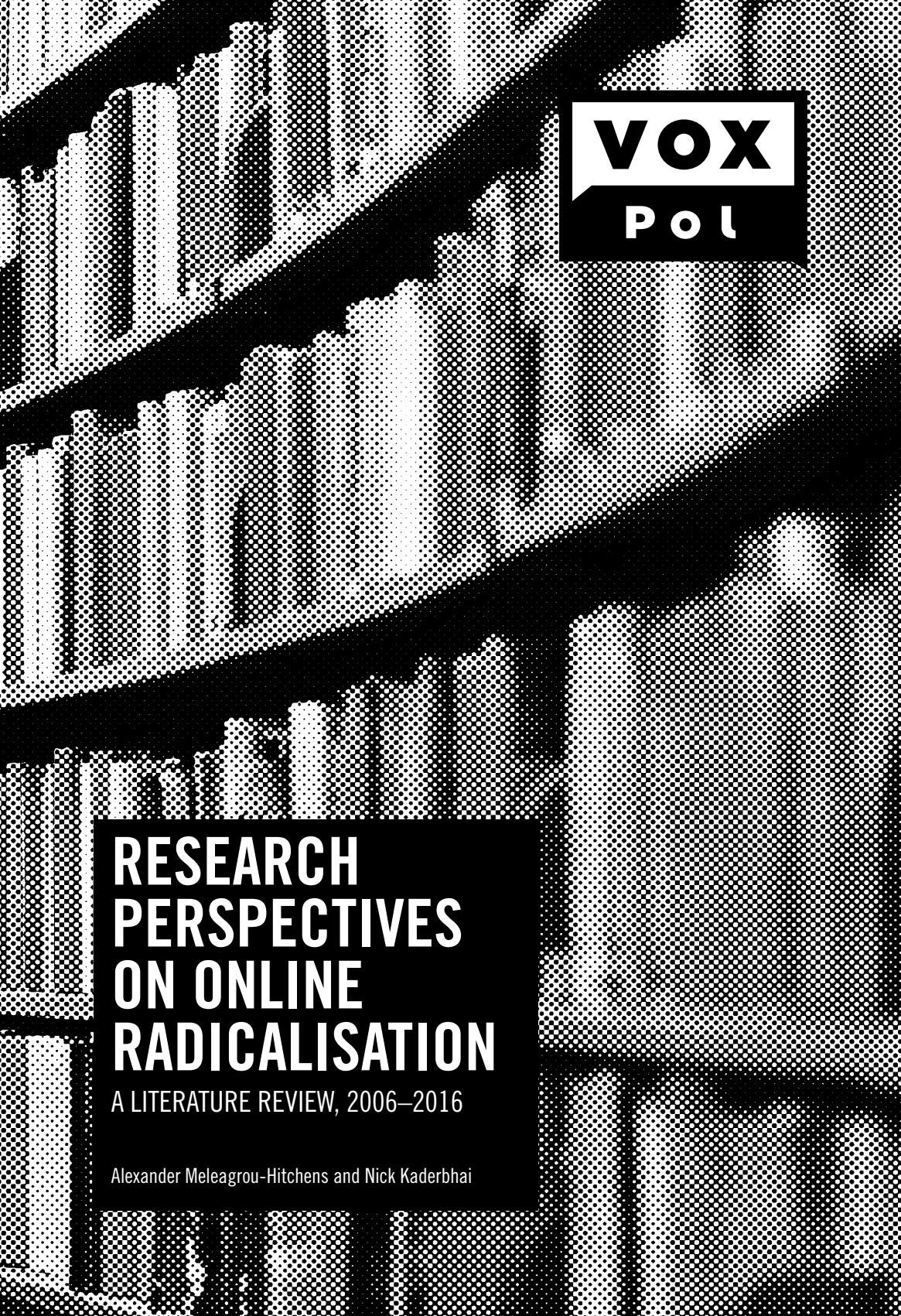


RESEARCH PERSPECTIVES ON ONLINE RADICALISATION

A LITERATURE REVIEW, 2006–2016

Alexander Meleagrou-Hitchens and Nick Kaderbhai

RESEARCH PERSPECTIVES ON ONLINE RADICALISATION

A LITERATURE REVIEW, 2006–2016

Alexander Meleagrou-Hitchens and Nick Kaderbhai
International Centre for the Study of Radicalisation (ICSR),
King's College London

About the authors

Alexander Meleagrou-Hitchens (PhD) is currently Research Director at the Program on Extremism at George Washington University. He was previously Head of Research at the International Centre for the Study of Radicalisation (ICSR) at King's College London, a VOX-Pol Researcher and a lecturer in the King's Department of War Studies.

Nick Kaderbhai is an Associate Fellow at the International Centre for the Study of Radicalisation (ICSR) at King's College London. He was previously a full-time Research Fellow, where he focused on the radicalisation and recruitment of western foreign fighters to extremist groups in Iraq and Syria. He is currently a doctoral candidate in the Department of War Studies at King's College London, where his is studying the interplay between British grand strategy and national identity.

Acknowledgements

The authors are grateful to Professor Maura Conway and Lisa McInerney of Dublin City University and Professor John Bew of King's College London for their support and advice. We must also thank Christina Mitsiali of ICSR for her tireless efforts in proofreading the various iterations of this report.

ISBN: 978-1-873769-66-9

Designed and typeset by Soapbox, www.soapbox.co.uk

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This literature review seeks to recalibrate our understanding of online radicalisation, how it is conceptualised within the literature and the extent to which the policy debate has advanced in response to technological and legal developments. Among the findings are the following:

- In recent years, the overwhelming focus of this avenue of research has been on the global jihad movement. This is therefore reflected in the review, but an effort has also been made to highlight similar research on other movements;
- As with the wider debate on radicalisation, there is little agreement on what constitutes online radicalisation and how, if at all, it happens. The influence of online interactions and propaganda on processes of radicalisation therefore remains a highly contested subject. It is a topic that has produced a broad swathe of literature, using different methodologies from a variety of disciplines;
- Consensus is that the Internet alone is not a cause of radicalisation, but 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 negatively impacted on the strength of research on this topic. Nonetheless, the exponential rise in violent extremist use of social media platforms has been the catalyst for an increase in research on the topic, and has begun to provide researchers with new forms of primary source data;
- Extremist use of the Internet has rapidly evolved and effectively adapted to a constantly shifting online media environment. Indeed, organisations – both public and private – that seek to respond to this are still playing catch-up, and have yet to mount a convincing response;

- One of the most celebrated aspects of social media – its ability to tailor content that appears on users' feeds that appeals to their specific values and interests and plugs them into networks of like-minded individuals – is also what makes it a key asset for extremist groups. Both in the physical and virtual realm, such groups rely heavily upon isolating potential recruits from views and opinions that diverge from their prevailing ideologies and narratives. Extremists seek to insert people into echo chambers that amplify their message and suppress any contrary opinions. Thus, by its very nature, social media creates for its users an environment that, in some cases, is conducive to radicalisation. This is neither a criticism of social media companies nor a call for them to fundamentally change the services they provide, but rather a comment on the complexity of the challenge of online radicalisation;

- While some analysts and scholars call for measures such as censorship, others argue that softer approaches, such as creating online so-called 'counter-narratives' and educating Internet users, would be more effective. However, it is clear that there remains both a lack of understanding of how this would occur, or how such narratives could be effectively disseminated. While very few studies provide a convincing explanation of either, there are signs that a more sophisticated approach is beginning to take shape.

INTRODUCTION

Since its inception and subsequent widespread use, the possible utility of the Internet for extremist groups' expansion and recruitment has not been lost on their leading figures and strategists. In the first instance, it has primarily been seen as a valuable communication tool that enables extremist non-state actors to take more direct control of their propaganda and media output, allowing them to bypass mainstream media that they perceive as biased and part of the conspiracy that they believe they are resisting.

As early as 1998, the figurehead of America's white supremacist movement, David Duke, wrote that the Internet would help to "facilitate a worldwide revolution of White awareness", while also helping the movement reach its audience directly rather than through the mainstream media (Anti-Defamation League (ADL), 2001). In 2004, Abu Bakr Naji, whose work on Jihadist strategy has been cited as a key influence on the self-proclaimed Islamic State in Iraq and Syria (ISIS), wrote in his seminal text, *The Management of Savagery,* that in order to succeed, the global jihad movement had to increase efforts to create its own, alternative sources of media. This would not only allow the movement to present itself in the best possible light, but could also help it combat and undermine the invincible and altruistic image he believed the West had cultivated for itself through mainstream media (Winter, 2015:41). Similarly, in 2006, global jihad strategist Abu Mus'ab al-Suri wrote in his treatise on how to expand al-Qaeda's global outreach and recruitment programme that the "informational resistance" against the perceived Western war on Islam must be "conducted through the use of modern technology of all forms, especially satellite and the Internet, to promote the resistance and entice people to action" (al-Suri, 2006:857).

While it is undeniable that extremist groups of numerous stripes have identified the Internet as an important tool, the precise impact of their use of this medium remains unclear. The effect of the

Since its inception and subsequent widespread use, the possible utility of the Internet for extremist groups' expansion and recruitment has not been lost on their leading figures and strategists.

Internet and online interactions on processes of radicalisation and recruitment, therefore, remains the focus of vigorous debate. Both the spread of home-grown terrorism in the West and the influx of foreign fighters into the Levant saw a surge of research interest in the topic, as analysts attempt to gauge how the Internet has contributed, if at all, to these problems. It is important to realise, however, that violent non-state actors' use of cyberspace is not unique to, and did not begin with, the global jihad movement; American neo-Nazis first realised the potential of the medium as early as 1983 (Michael, 2013:42). Intending originally to encourage ideological debate, pool resources and create a "virtual networked community", radicalisation was not considered by extremists as the Internet's primary use at that time (Levin, 2010:960). The medium increasingly began to inspire the message however; when groups started to call for lone-actor attacks, the Internet provided the platform through which participants could take their cues. As the success of the approach became clear, similarly aligned movements realised that online activity had usurped the influence of veteran ideologues in drawing in sympathisers (Brachman & Levine, 2011). Accessibility trumped ideological authority, and group dynamics that perpetuated radicalisation and recruitment could perhaps now be mirrored online.

This literature review is an attempt to provide an up-to-date assessment of how online radicalisation is currently understood. In doing so, it will:

- Reveal the continuing disputes regarding the conceptualisation of radicalisation generally and online radicalisation specifically;
- Illustrate how the so-called 'Jihadisphere' and other online extremist communities (Conway, 2012:4; Ducol, 2012:51–52) emerged out of the platforms created by the evolution of Web 2.0 and the extent of their influence on radicalisation;

- Discuss the various types of violent extremist materials available online, and the diversity of platforms on which they are shared;
- Discuss how scholars, analysts, governments and private companies have developed policy recommendations and strategies for countering the use of the Internet by violent non-state actors.

That no unified theory of radicalisation exists is a truism, as is the fact that the relationship each individual has with online content and networks is unique. This has allowed academics from a variety of disciplines to assert their particular angle on the topic (with varying levels of success), and serves as a key motivation behind the production of this review.

Before delving into the literature, a few caveats are worth mentioning. Most of the literature on online radicalisation comes in the form of books, journal articles, reports and testimony from governmental hearings. While journalists have made some interesting interventions into the debate (Reitman, 2013; Callimachi, 2015, 2017; Griffin, 2015) their work is referred to largely for matters of context. Second, the literature tends to fall into two camps: the far right; and the global jihad movement. Efforts have been made to reflect this in the review. However, the majority of the literature, including material related to policy, examines online jihadist radicalisation. Third, the subject is embedded within a diverse array of disciplines, methodologies and data. Much of the material naturally overlaps with more general discussions of radicalisation, and it is therefore instructive to first provide a brief discussion of current understandings of radicalisation. Once these have been established, the review will move on to explain how scholars and analysts view the influence of the Internet on this phenomenon.

DEFINITIONS AND PROCESSES OF RADICALISATION

IN ITS ORIGINAL form, the term 'radicalisation' appeared in academic literature as a general way of describing a person's or a group's move towards more radical politics. While some argue that this is where it should have stayed (Jones & Smith, 2015), the term took on new meaning following the spread of home-grown jihadism in the West after the September 11, 2001 attacks. It is now widely used to refer to the process of individuals joining extreme or violent political movements, with contemporary emphasis on the recruitment and mobilisation of Western Muslims to the cause of global jihad.

Scholars such as Arun Kundnani have (somewhat conspiratorially) argued that the term's more recent application is part of a cynical ploy by academics to gain funding from Western governments by detracting from the true 'root causes' of terrorism, such as poverty and Western foreign policy (Kundnani, 2012:5). On the contrary, setting aside the arguable misuse of the term 'radical', as we shall see, the study of radicalisation represents an attempt to provide a more nuanced understanding of the causes of political violence in the West that go beyond such simplistic explanations. While taking into account the grievances that scholars like Kundnani believe are the sole explanation, the term is used to refer to how grievances and ideas, and the way that these are operationalised by terrorist recruiters, have an impact upon a gradual, individual-level process of embracing violent extremism. It is therefore instructive at this point to briefly discuss how radicalisation has been defined by governments and academics.

As demonstrated by, among others, Della Porta and LaFree, there is no agreed upon definition of radicalisation. Existing definitions include:

- "a process leading towards the increased use of political violence";
- "the strategic use of physical force to influence several audiences";
- "increased preparation for, and commitment to, intergroup conflict";
- "an escalation process leading to violence" (Della Porta & LaFree, 2008:4–10).

McCauley and Moskalenko also provide a useful way of dividing our approach to understanding radicalisation when they write that:

> Functionally, political radicalization is increased preparation for and commitment to intergroup conflict. Descriptively, radicalization means change in beliefs, feelings, and behaviors in directions that increasingly justify intergroup violence and demand sacrifice in defence of the group (McCauley & Moskalenko, 2008:416).

Noting the existence of such "heterogeneous definitions" while directly referencing Della Porta and LaFree's findings, Schmid concludes that radicalisation is "a very problematic concept" (Schmid, 2013:6). Given the deep and politicised divisions over the causes of the terrorist threat to the West, such confusion and debate over the term is likely to continue.

Among the main fault lines in this debate is the connection between radicalisation and violence. Some definitions present it as an adoption of extremist ideas that reject normative, liberal values, while calling for far-reaching changes to society that may or may not lead to violent action (AIVD, 2006; PET, 2008; RCMP, 2009). Others refer to 'violent radicalisation' in order to emphasise the violent outcome, thus distinguishing the process from non-violent forms of extremism (Neumann & Stevens, 2009:10; Ranstorp, 2010; House of Commons, 2012).

Another set of definitions come from governments that, over the last decade, have developed strategies aimed at curbing the threat from domestic and/or home-grown terrorism. The Danish, Swedish, British and Dutch governments provide the most frequently cited of these. According to the Danish Security and Intelligence Service (PET), radicalisation is "a process, by which a person to an increasing extent accepts the use of undemocratic or violent means, including terrorism, in an attempt to reach a specific political/ideological objective" (PET, 2008:1). Similarly, the British Government describes it as "the process by which a person comes to support terrorism and forms of extremism leading to terrorism" (House of Commons, 2012:3). Both of these definitions conceive

of the adoption of extremist ideas *and* violence as components of the radicalisation process. In the definition provided by the Dutch General Intelligence and Security Service (AIVD), however, violence is not seen to be as crucial: "radicalisation is the pursuit of and/or support for far-reaching changes in society which may constitute a danger to the democratic legal order, which may involve the use of undemocratic methods that may harm the functioning of the democratic legal order" (AIVD, 2006:13).

Most scholarly definitions, on the other hand, focus on violence as a central component of radicalisation. Neumann and Rogers, for example, describe radicalisation as a process of "changes in attitude that lead towards sanctioning, and ultimately, the involvement in, the use of violence for a political aim" (Neumann & Rogers, 2007:11). McCauley and Moskalenko provide a more nuanced description, referring to "political radicalisation" as "changes in beliefs, feelings and behaviour in the direction of increased support for a political conflict" (McCauley & Moskalenko, 2011:82). They then note, contentiously, that radicalisation can "involve the movement of individuals and groups to legal and nonviolent political action (activism) or to illegal and violent political action (radicalism)" (McCauley & Moskalenko, 2011:82). Finally, they define terrorism as simply the most extreme version of radicalisation "in which a non-state group targets not only government forces but civilian citizens supporting the government" (McCauley & Moskalenko, 2011:82).

Existing theories and models related to the causes of radicalisation in the West offer a variety of explanations. Many of these theories are divided between those that focus on either a top-down or bottom-up process, with both taking into account the effect of the Internet. Top-down approaches tend to focus on what they see as the critical role of the external radicaliser, often a recruiter for a terrorist group or a religious figure with extremist sympathies (PET, 2008; Hoffman, 2008, 2010). This relationship then sparks a series of changes within an individual's behaviour, such as the rejection of relationships with friends and family in favour of a more puritanical moral code, which eventually leads to them

joining a violent extremist group and/or carrying out an act of violence. Bottom-up theories instead argue that an individual's radicalisation derives from one's interaction in physical social networks (Sageman, 2004; Bhatt & Silber, 2007). This, in turn, leads to an exploration of extremist ideologies within peer groups, the intensification of beliefs and the creation of a feeling of duty to take part in extremist activity, including violence. In addition, a number of both top-down and bottom-up theories provide sequential or stage-based models that present radicalisation as a linear progression (Borum, 2003; Moghaddam, 2005; Bhatt & Silber, 2007; Precht, 2007). However, it is the theories that avoid both the sequential approach and the strict division between bottom-up and top-down that are perhaps the most comprehensive and convincing (Wiktorowicz, 2005; Veldhuis & Staun, 2009).

Being a member of a tightly-knit clique of like-minded individuals connected through a wider social network is far more important, some argue, than the embrace of ideology or the outreach being made by propagandists online.

Despite varying approaches in the radicalisation discourse, it is possible to identify the most regularly cited causes of radicalisation in the West. Many authors place great significance on the role of *physical, face-to-face interactions within social networks* (Sageman, 2004, 2008), an ingredient that is vital "for this development to foster and propagate" (McFarlane 2013:2).

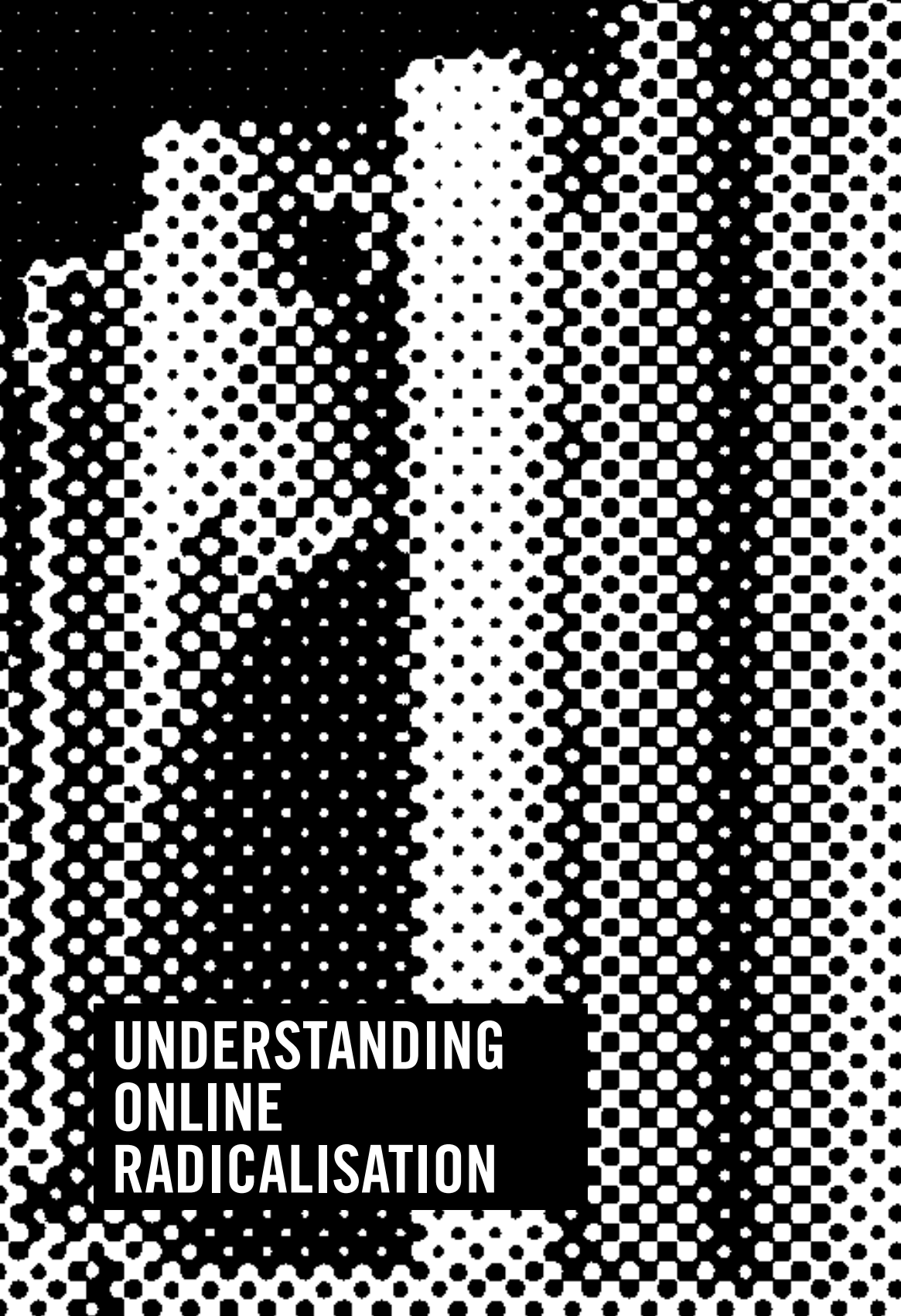
Being a member of a tightly-knit clique of like-minded individuals connected through a wider social network is far more important, some argue, than the embrace of ideology or the outreach being made by propagandists online. This is linked to the process of *socialisation,* or an individual's gradual adoption of norms, ideologies and customs that stems from their involvement in a certain social group, that some authors focus on as a major contributing factor (Wiktorowicz, 2005).

Studies also emphasise the role of *ideology* and its appeal to Westerners, with some citing this as among the most important components of home-grown radicalisation and terrorism (NYPD, 2007; Hoffman, 2008; PET, 2008; Meleagrou-Hitchens, 2011). Referring

to the case of Colleen LaRose, Halverson and Way point out that it was not so much the content of the ideology that proved influential, but rather what the ideology represented, namely "social beliefs, norms, practices and techniques" that could be applied and give meaning to a life of exclusion (Halverson & Way, 2012:145). In this instance, the global jihadist ideology "provided an increasingly accessible… framework for critiquing Western thought and resisting the social order" (Halverson & Way, 2012:145).

Most studies also place varying degrees of importance on the role of *identity*, and suggest that an identity crisis and the subsequent manipulation of this by violent extremists is often one of the first steps in the radicalisation process (Silke, 2008; Wiktorowicz, 2005; Venhaus, 2010). The role of *leadership figures and propaganda* also feature prominently in many radicalisation theories, with the legitimacy of the former having a significant impact upon the efficacy of the latter. Thus, while a message from a violent extremist group may be convincing to its target audience on its own, it is far more powerful when presented by an individual or group that the audience regards as a legitimate, authoritative and a trusted source. The audience must also be considered as active participants in the "process of message transfer" (Aly, 2009:2), and Archetti reminds us that information simply being "out there" is not enough – the availability of a message does not necessarily equate to its reach (Archetti, 2015:50).

It is worth noting here that none of these models and theories should be seen as *the* explanation for radicalisation, but rather as useful insights into factors for consideration when trying to understand this phenomenon. As the focus of this review is the role of the Internet, the following sections unpack and assess views on how it impacts on processes of radicalisation.


UNDERSTANDING
ONLINE
RADICALISATION

THIS SECTION FOCUSES upon works that have attempted to further our understanding of the relationship between media communications and violent radicalisation. As with the wider debate on radicalisation, there is little agreement on what constitutes online radicalisation and how, if at all, it happens. The influence of online interactions and propaganda on processes of radicalisation therefore remains a highly contested subject. Similarly, scholars are still grappling with the question of how much the Internet can act as a replacement for physical interactions and if, in turn, online networks are able to have the same influences upon an individual as real-world social and kinship networks.

As we shall see, 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. Nonetheless, the exponential rise in violent non-state actors' use of social media platforms has been the catalyst for an increase in research on the topic, and has begun to provide researchers with new forms of primary source data.

NEW MEDIA AND THE IMPACT OF CONNECTIVITY IN THE MODERN WORLD

In an effort to better understand the influence of the Internet and media on radicalisation, some scholars have chosen to focus more on how the term is perceived by mainstream audiences and how it is influenced by modern media. Awan et al. provide the most comprehensive analysis of this, and argue that the way in which we perceive radicalisation in the first instance has been altered by what they describe as the "new media ecology", among the characteristics of which is so-called "mediatisation" (Awan et al., 2011:5). To help clarify, they draw on the work of Hjarvard who defines the new media ecology as the public's increasing reliance upon the media's presentation of the world due to its integration into existing social institutions and supposed status as a social institution in its

own right (Hjarvard, 2008:113). An example of this would be what Nacos describes as "the triangle of political communication" in which the media acts as a critical yet active tool that has the ability to enhance or diminish stories and ideas surrounding the discussion of terrorism and terrorist attacks (Nacos & Torres-Reyna, 2007).

This has greatly affected social interactions, which now take place through media in various forms. Many facets of modern life are perceived as being "dependent upon media, and have been transformed to increasingly follow media logics" (Awan et al., 2011:5). The authors conclude that this has affected how the public views the threat from radicalisation. Thus, while the study is concerned with how jihadist propaganda and other messaging can have an impact on radicalisation, it also seeks to shed light on the discussion of the term itself, how it is presented within the modern media apparatus and the possible negative impact this is having.

However, this "new media ecology", or how the real and virtual worlds synthesise, has yet to be fully understood or conceptualised. Awan et al. define the phenomenon as "the current rapidly shifting media saturated environment characterized by a set of somewhat paradoxical conditions of, on the one hand, 'effects without causes' … yet, on the other, as profound connectivity through which places, events, people and their actions and inactions, seem increasingly connected" (2011:5). These "patterns of connectivity" have, according to the authors, allowed groups to create and disseminate inflammatory imagery and propaganda over various platforms. Accordingly, such a condition is brought about due to the increased connectivity and interaction facilitated by new media, especially the Internet. The key actors in radicalisation, according to this study, are the producers of jihadist material online, the mainstream media covering this phenomenon, and the audiences that consume both. Through the interactions among these three agents, a "number of discourses (on and of radicalisation) and a range of experiences (fear, anxiety, mistrust, uncertainty) emerge via a diffused information infrastructure" (Awan et al., 2011:124). Their study is therefore divided along the following three lines: forms of Internet communication (such as websites, blogs, and social networks) used

by violent non-state actors to radicalise individuals and encourage violent acts; the mainstream media's portrayal of radicalisation and the terrorist threat to the West; and how the views of mainstream audiences on the meaning and threat of radicalisation are influenced by the media (Awan et al., 2011).

Through their findings they argue that, while online jihadist activity – such as the dissemination of jihadist ideology in various languages (for more see Condon & Weyers, 2014) – is helping to push people towards violence, "uncertainty about how discourses of radicalisation operate in the new media ecology is the condition for discourses about radicalisation to proliferate" (Awan et al., 2011:7). Put simply, they posit that the media and its approach to the radicalisation phenomenon has contributed to the "securitisation" of life in Britain in which a "media-security nexus" made up of politicians, commentators and their audiences, creates an atmosphere of fear and suspicion towards Muslims.

A drawback of this study, however, is that the part of this research exploring the impact of media on public understandings of radicalisation was based on a small, unrepresentative sample of 67 participants who were also "part of the social networks of our team of ethnographic researchers, with further participants recruited through snowballing" (Awan et al., 2011:17). Nacos rightly observes that this "seems questionable for assembling a cross section of regular citizens" (Nacos, 2011:476).

A related study (O'Loughlin et al., 2013) also identifies a dearth of reliable profiles of radicalised individuals and argues that much of the mainstream media contributes to an increasing vagueness of what constitutes radicalisation. This, according to the authors, "contributes to a sense of a persistent but diffused and underspecified threat, a state of 'hypersecurity'" (O'Loughlin et al., 2013:155). For Hoskins and O'Loughlin, that the discourse is misappropriated by the politico-media nexus makes terms such as 'radicalisation' troublesome, covering up a trajectory of "alienation and preventing engagement with root-causes" (Hoskins & O'Loughlin, 2009:107). Such is the effect of this conceptualisation that the "threat posed by and the pursuit of so-called 'online radicalization' and the

online/offline distinction make little sense" (Hoskins & O'Loughlin, 2009:108–109). Gill et al. endorse the idea that this is a "false dichotomy" via the simple fact that "plotters regularly engage in activities in both domains", and that such a conceptualisation represents "two extremes of a spectrum that regularly provide prototypical examples in reality" (Gill et al., 2015:35). The more interesting investigation for these authors is thus not online versus offline, but rather "interactions with others" versus "no interaction with others" (Gill et al., 2015:35).

COMMUNICATION TOOL OR DIRECT FACILITATOR?

Among the earliest references to the importance of the Internet in the recruitment of individuals into extremist groups comes from two of the leading figures in the fields of terrorism and radicalisation studies: Bruce Hoffman and Marc Sageman. Indeed, their differing positions on the role of the Internet represent one of the main divides in the wider discussion of this topic: whether the Internet plays a role simply as a means to communicate radicalising propaganda, or if it can also help to create, or at the very least act as a support mechanism for, violent extremist networks.

As outlined above, Hoffman focuses on top-down processes of radicalisation that elevate the importance of hierarchical relationships above those of networks. He places emphasis on the role of individual and external recruiters and 'radicalisers' who form part of a hierarchical set-up like, for example, al-Qaeda Central. Focusing on the use of new media and the Internet by al-Qaeda recruiters, he understands radicalisation as a process primarily influenced by the messaging efforts of global jihadist leadership figures. He argues that, "from the start its [al-Qaeda's] leadership seems to have intuitively grasped the enormous communicative potential of the Internet and sought to harness this power both to further the movement's strategic aims and facilitate its tactical operations" (Hoffman, 2006:5).

The Internet thus offered al-Qaeda three crucial functions, which have been previously articulated in a range of ways in different contexts (Furnell, 1999; Cohen, 2002; Lee & Leets, 2002; Thomas, 2003; Weimann, 2004): propaganda, which allows for recruitment

and fundraising; terrorism-related training and instruction; and the provision of a vast array of open source information channels that are useful for planning and executing terrorist attacks. Mahmood has recalibrated the framework again since the social media age, but largely retained the content, identifying recruitment, glorification and propaganda, planning and information, target selection, training and fundraising as the key goals of extremist groups using online social networks (Mahmood, 2012:574).

Hoffman narrows his analysis to al-Qaeda's ideological, tactical, and strategic output via the Internet. He is particularly attentive to online global jihadist magazines such as *Sawt al-Jihad*, which emerged in 2004 carrying a "message that was less one of attacking US and other Western targets than the importance of mobilizing Muslim public opinion and support of jihad" (Hoffman, 2006:9). Violent radicalisation and recruitment, in this analysis, are dependent upon effective communication which "ensures the continued flow of fighters into the movement, bonding supporters more tightly to it, and drawing sympathizers more deeply into its orbit" (Hoffman, 2006:15). However, much like other popular and widely cited theories, Hoffman's 2006 work is limited in that it pre-dates the more recent developments of individuals carrying out attacks without any direct connection to the organisations that they claim to act on behalf of. His theory is based on the notion that people are drawn to and join formal organisations primarily due to their outreach and recruitment efforts, whereas we now see that joining a formal group is no longer a prerequisite for involvement in terrorism (Bergen et al., 2013).

Marc Sageman, on the other hand, has provided what is perhaps the most popular bottom-up theory in his book, *Understanding Terror Networks* (2004). Sageman uses social network analysis to argue that al-Qaeda is a network brought together by (and heavily reliant upon) personal relationships. While he places some emphasis on the role of ideology and its dissemination via the Internet, the most important factor for those joining the global jihad movement, he argues, is their involvement in a friendship or kinship network with connections to senior al-Qaeda recruiters (Sageman, 2004). In his follow-up work, *Leaderless Jihad* (2008), Sageman furthers

the argument by reducing the importance of the role of senior recruiters, noting that al-Qaeda Central's role has been subsumed by the global social movement it helped to create. Instead, he contends that networks now form at a grass-roots level and carry out operations without the need for any form of oversight from al-Qaeda or any other formal, hierarchical group. The radicalisation process is therefore born out of face-to-face interactions based on friendship and kinship.

Sageman contends that the Internet has breathed new life into the process, assisting in the creation of networks and allowing for the provision of "general guidelines" that act as a "virtual glue" (Sageman, 2008:144). This then allows for the creation of a "leaderless jihad". The Internet also creates the conditions for a minimal level of ideological, strategic and tactical coherence, allowing al-Qaeda Central to advertise "demands for terrorist operations on the Internet" (Sageman, 2008:144). Sageman presents this virtual world as a sort of marketplace which "coordinates the distribution of goods and services in a country" but which no one is in charge of: "Each buyer or provider pursues his or her own interest, but the overall pattern is that everyone is fed, housed, and clothed. The coordination is generated spontaneously from the bottom up, through the 'invisible hand' of the market" (Sageman, 2008:145).

Winter echoes this sentiment, albeit in a slightly different way, suggesting that social media has emerged as "the decade's radical mosque" (Winter, 2015:7). Weimann concurs, writing that the "interactivity, reach, frequency, usability, immediacy and permanence that the virtual world has come to provide now heighten and mimic those processes that took place previously inside places of worship" (Weimann, 2014:2). Indeed, Koehler's interviews with former German far-right extremists reveal a belief among them that, while the Internet created an effective and efficient space in which to interact, they only felt truly part of the movement after attending rallies and meeting members in the real world (Koehler 2014:123). Thus, while offline, face-to-face interactions and involvement in networks are still central to Sageman's theory, he does concede that the Internet plays an important, albeit secondary, role, with more recent studies produced since tending to back this up.

Taking this idea of the Internet as a replacement for real-world physical spaces further, Torok conceptualises the Internet as an institution in the Foucauldian sense. Due to traditional institutions, such as training camps, becoming increasingly difficult to maintain because of military pressure, "terrorists have had to create new forms of institutions to recruit, radicalize and train" (Torok, 2013:1). According to her, the Internet is the "most significant" of these new institutions, and allows for the "gathering and coordinating" of individuals vulnerable to radicalisation (Torok, 2013:2). Such institutions, she argues, use "discourse and networked power relations in order to normalize thoughts and behaviours". This framework of power operates within the online environment and is used by extremists to "recruit and radicalize" (Torok, 2013:1).

The most convincing studies of online radicalisation also seek to temper what is seen as a tendency to over-emphasise the importance of media and the Internet in radicalisation processes.

The most convincing studies of online radicalisation also seek to temper what is seen as a tendency to over-emphasise the importance of media and the Internet in radicalisation processes. Benson, for example, begins with the simple point that, while access to the Internet has increased across the globe, it has not correlated with any increase in transnational terrorist attacks (Benson, 2014). This is supported by Gill et al., whose empirical study of individuals reportedly radicalised via the Internet found no connection between the rise of the Internet and the rise of lone-actor terrorist attacks between 1990 and 2011 (Gill et al., 2015). In his analysis, Benson examines and criticises what he refers to as the "causal logics" that have led to conventional wisdom about the Internet's role in this regard. Existing empirical approaches to the question are fundamentally flawed, he claims, due to their creation of a causal link between an individual's use of the Internet and their subsequent involvement in an act of terrorism. "It would be strange", he notes, "if today's terrorist did not use the Internet, just as it would be strange if past terrorists did not use the postal service

or telephones" (Benson, 2014:311). As an extension to this, Archetti also bemoans the common lack of historical perspective. What might be seen as an unprecedented "communication revolution" is "barely the latest manifestation of those profound changes that the introduction of *any* communication technology, from the invention of parchment, to the printing press and the telegraph, has always contributed to across the centuries" (Archetti, 2015:51).

That terrorists are engaged in online activities, while perhaps unremarkable, has also been tested empirically, and findings suggest that the Internet has also assisted in facilitating communications *among* like-minded extremist political activists. In one of the first such studies, Gill et al. drew from a database of 119 lone-actor terrorists and found that 35% of them used the Internet to interact with networks of like-minded political activists, while 46% used the Internet for didactic purposes related to their attacks (Gill et al., 2014:430). This study also found that, while the Internet certainly played a role in modern terrorism, it was a largely instrumental one; "whether it be pre-attack (e.g. surveillance, learning, practice, communication) or post-attack (e.g. disseminating propaganda)", the attacks were "cyber-enabled, rather than cyber-dependent" (Gill et al., 2015:28).

For Archetti, the effect of the Internet is also overemphasised by "technological determinists", who overlook the fact that it is always humans "who *use* technology as a tool to advance their own goals and that audiences, as already indicated, actively select and embrace – rather than merely absorb – messages they are interested in" (Archetti, 2015:50). The Internet, then, becomes "no more effective than the old-fashioned poster" (Archetti, 2015:50). The mere presence of Internet use, Benson concludes, does not in any way prove a causal link. In relation to this, Benson also makes the very salient point that most existing studies also lack independent and dependent variables that would include both the use of the Internet by terrorists and states, thus omitting negative cases which would help to "determine the net effect of the Internet on transnational terrorism" (Benson, 2014:312). Indeed, a lack of dependent variable samples within research

data is recognised as a methodological fault within the wider terrorism and radicalisation studies community, and one that very few studies into online radicalisation take into account. Among those scholars who do are Gill et al., whose dataset includes individuals who took part in violent activism but did *not* appear to engage in online activities (Gill et al., 2015:11).

Instead of helping terrorists, then, Benson argues that the growth of Internet use over recent decades has further empowered security agencies in their fight against terrorism, which gain "at least as much utility from the Internet as terrorist groups do" (Benson, 2014:293). While he acknowledges that a combination of anonymity, abundance of information, and ease of communication provided by the Internet could indeed be conducive to terrorism, he suggests that these qualities are equally detrimental to terrorists. This alludes to issues that will be covered in more detail below, such as the problem of trust in online communications (see Hegghammer, 2014). It also highlights the problem raised by Nesser that, while the Internet does provide a platform, it still requires credible and charismatic messengers (Nesser, 2010:108–110).

In his efforts to downplay the importance of the Internet, Benson goes even further when he claims that al-Qaeda was in fact stronger and more of a threat before becoming reliant on modern communication technologies. While one might assume that al-Qaeda's post-2005 decentralisation (for more see Borum & Gelles, 2005) would lead to increased operational flexibility and geographic scope, he argues that its attack capability has instead been eroded as a result, with "pre-Internet al-Qaeda" carrying out many more successful attacks (Benson, 2014:313). Indeed, even attacks that do appear to have been at least partially inspired by Internet activity have tended to lack effectiveness and lethality. Focusing specifically on home-grown terrorism, Benson acknowledges some degree of causal effect with Internet use while maintaining that most such cases had more important influences, such as psychiatric disorder. He identifies the 2013 Boston Marathon bombing as an incident that appears to present the most convincing case for the Internet's influence over a terrorist act. Yet even here he points out that "the Internet appears

to have been one influence among many" (Benson, 2014:316). In keeping with his core argument cited above, Benson hastens to point out how useful the Internet was to authorities in allowing them to track down the attackers and prevent further attacks.

Another aspect to consider when evaluating the importance of the Internet as a possible direct facilitator of radicalisation is the vulnerability of the individual and the extent to which they are predisposed to radicalisation before using online platforms. Durodie and Ng, for example, argue that no individual approaches the Internet in isolation, rather "they come to it already bearing a vast number of ideas, assumptions and emotions" (Durodie & Ng, 2008:2). Thus, for some, a greater focus on the root causes of radicalisation must be given greater importance than the medium of the Internet (Githens-Mazer & Lambert, 2010). For these authors, the Internet is largely seen as a medium to communicate content and ideology and, while important, is neither novel nor deserving of such an inflated reputation for facilitating radicalisation (Mealer, 2012:10). An example often cited is that, although the 7 July, 2005 London bombers were said to have been influenced by online videos, they were also influenced by their mass media consumption (Kirby, 2007).

For some authors, so-called 'self-radicalisation' (or radicalisation in isolation from wider networks) and radicalisation over the Internet are one and the same (Behr et al., 2013:20). This is a novel view, however, as very rarely do scholars categorically state that the Internet alone has the power to 'self-radicalise' an individual, thus implicitly accepting the premise that the radicalised individual had little chance of radicalising without it, or that the process was solitary or solely based on the consumption of online media (Kirby, 2007; ADL, 2014). It must also be remembered that in some countries, such as Indonesia, online propaganda acts as an add-on to the already ubiquitous offline literature that is available (Yasin, 2011:1). Nonetheless, Kirby does state that the "self-starter" phenomenon has been seriously affected by the rise of the Internet (Kirby, 2007:416).

The ADL is another source that strongly asserts the 'self-radicalisation' phenomenon, stating that "face-to-face interaction with terrorist operatives is no longer a requirement for

radicalisation". Individual extremists, or lone actors, are therefore "increasingly self-radicalising online" (ADL, 2014:1). In a study conducted by the Southern Poverty Law Center about the popular American white nationalist online forum Stormfront, the author found that "registered Stormfront users have been disproportionately responsible for some of the most lethal hate crimes and mass killings since the site was put up in 1995" (Beirich, 2014:2). However, while it provides interesting anecdotal accounts of forum users who went on to commit racially motivated violent crimes and murder, little effort is made to explain how and why supporters of white-supremacist violence on Stormfront graduate from online engagement with the movement to violent activism. In providing a profile of the typical Stormfront user who moves on to violence, the report offers only the following by way of explanation, omitting any inquiry as to why some move on to violence while others are content to restrict their activity to the Internet:

> Assured of the supremacy of his race and frustrated by the inferiority of his achievements, he binges online for hours every day, self-medicating, slowly sipping a cocktail of rage. He gradually gains acceptance in this online birthing den of self-described "lone wolves," but he gets no relief, no practical remedies, no suggestions to improve his circumstances. He just gets angrier. And then he gets a gun (Beirich, 2014:1).

For Ravndal, the case of far-right terrorist Anders Behring Breivik supports this approach. While acknowledging that "no one will ever know for sure" whether Breivik would have turned to violence without the Internet, Ravndal argues that it was decisive in Breivik's trajectory, "influencing his disposition to engage in actual mass murder" (Ravndal, 2013:182). It created a new reality in which Breivik's views went uncontested, and provided tactical training and online games that isolated him from the outside world. Weimann broadly agrees, but pushes back against claims that the process is completely solitary. Individuals are never completely out of contact and "they connect, communicate, and share information, know-how, and

guidance exclusively online" (Weimann, 2014). A combination of this contact with extremist propaganda and online discourse can, according to him, have a profound effect upon the radicalisation of lone actors and inspire them to commit their violent acts (Weimann, 2014).

This is supported by Gill et al., who note that, while not causing an increase in the number of attacks, the Internet has certainly altered individuals' means of radicalisation and attack learning (Gill et al., 2015). The authors also list a number of novel characteristics regarding lone actors' use of the Internet, including that offenders who interacted virtually with co-ideologues were significantly less likely to successfully carry out a violent attack. Ultimately, these conclusions match those of Behr et al. in that the Internet enables radicalisation, but does not cause it (Behr et al., 2013). The strength of both of these studies comes from their empirical, case study driven approaches that rely on rich datasets, rather than the anecdotal over-reliance on secondary sources and conjecture that persists within the discipline. Lastly, it is important to note that the ADL does not distinguish between self-radicalisation (little to no networks) and radicalisation over the Internet. Rather, its report explains how past models that focused on offline peers and spiritual sanctioners as the key facilitators of the process (Bhatt & Silber, 2007) have now been usurped by the Internet as the dominant radicalising factor (ADL, 2014:2).

The above-mentioned case of Colleen LaRose is offered by Halverson and Way as a prime example of how offline socialisation is not necessarily a factor in an individual's radicalisation, thus challenging the view of many experts that "the Internet can support and facilitate but never completely replace direct human contact and the ties of friendship and kinship" (Halverson & Way, 2012:140). LaRose allegedly "never set foot in a mosque, kept no religious books, hung no religious images or symbols in her apartment, and, according to several of her neighbours, never spoke about her religious beliefs" (Halverson & Way, 2012:143). Similarly, a number of authors have pointed to the radicalisation of Roshonara Choudhry – who attempted to murder her local MP Stephen Timms in 2010 due to his past support for the UK invasion of Iraq – as an exception to the rule

(Gill et al., 2015; Pearson, 2015; McFarlane, 2010). Gill et al. tell us that she "bucks the trend" of the cases they analysed in that she appeared to be a true lone actor, and adopted an extremist ideology "in the absence of co-ideologues in the physical world" (Gill et al., 2015:27). Pearson agrees, claiming, "her attack on Timms appeared to be the result of a solitary online radicalization, contrasting with understandings of radicalization as a collective real-world phenomenon" (Pearson, 2015:2). For Park and Suyin, the case of Muhammad Fadil Abdul Hamid is another illustration of this apparently rare phenomenon (Park & Suyin, 2010). Hamid became exposed to extremist religious ideologies before attempting to contact Anwar al-Awlaki and a suspected al-Qaeda recruiter with the "hopes of undertaking militant jihad in places such as Palestine, Iraq and Afghanistan" (Park & Suyin, 2010:1).

While these cases are considered by some to represent exceptions that prove the rule (Mealer, 2012:57; Gill et al., 2015; Pearson, 2015), not enough research has yet been conducted to either support or invalidate the 'Internet-only' hypothesis. The literature on online radicalisation has since moved on, and the vast majority of authors argue that, while the Internet plays a facilitating role, in most cases the individual must still also be in contact with real-world networks. An investigation into an individual's trajectory is thus often an investigation into the unique interplay between online and offline interactions.

Related to this, engagement solely through online networks can serve to make potential recruits feel emancipated, both socially and cognitively. Social aspects of "in-group love" (Sageman, 2004, 2007) explain how individuals can feel a sense of belonging and identity for the first time, and how this, along with identifying out-groups that represent a direct threat, can be a strong pull towards the radicalisation process. Douglas explains how, in the case of the far right, this can happen through the "socially creative" designation of the white in-group as high status in relation to an out-group conspiring to cause its destruction, such as Jews and African Americans (Douglas et al., 2005:73). This is not to say that identity is monolithic; the Italian far right's virtual community has significant cleavages and segmentation, while the panorama of the non-party extreme right is also highly

fragmented and constantly evolving (Caiani & Parenti, 2010:286). Nonetheless, psychological mechanisms within groups can also arguably be implemented and facilitated within the online sphere (Sageman, 2004; Neumann, 2012:18). Furthermore, propagandists, through the nuanced use of old grandiose discourse (Gerdes, 2012; Conway, 2014) and behavioural affirmation (Neumann, 2012:18), make the individual feel included and enhance a sense of mission and self-importance (Bergin et al., 2009; Hui, 2010; Bjelopera, 2013). Neumann in particular focuses on how the Internet can catalyse self-idealisation, projecting the traits and characteristics that the individual aims to possess (Neumann, 2012:19).

The online works of English-speaking jihadist ideologues, such as Anwar al-Awlaki, are also argued in some cases to have provided the ideological support to allow for the adoption of new identities and online self-radicalisation (Bjelopera, 2013; Brachman & Levine, 2011). Among Awlaki's contributions to jihadist strategy was his effort to widen the parameters of involvement in the global jihad movement beyond direct physical recruitment and engagement in violence. In an attempt to increase the movement's support base, he sought to lower the bar for involvement by giving near-equal significance to other forms of jihad, such as the online dissemination of jihadist propaganda (Meleagrou-Hitchens, 2011). Now, Muslims could see and present themselves as members of the movement simply through online activism, and this too, it is argued, can contribute to radicalisation.

Awlaki's use of the Internet also made him more accessible to his followers, helping facilitate their radicalisation.

Awlaki's use of the Internet also made him more accessible to his followers, helping facilitate their radicalisation, and Archetti argues that such imagined relationships could not exist without the necessary communication technologies:

> Communication technologies, in this respect, can further extend our social reach in forming both direct relationships (through emails, for example, or by having a chat over the phone) and in building indirect relationships. For instance, an activist can develop an indirect relationship with an admired political figure (e.g. a terrorist leader) one comes to know through speeches available online. In this sense relationships can be *imagined* (Archetti, 2015:52).

In their study on Awlaki's role in elevating the online jihad to a level of prestige close to that of physical jihad, Brachman and Levine use the case of American convert Zachary Chesser. They demonstrate how he first undertook what he understood to be online jihad through his extensive online activism in support of global jihadism. Chesser took this upon himself after consuming Awlaki's work which explained to him that, while violent jihad was the pinnacle of movement activism, spreading propaganda was also vitally important. Nonetheless, the lure of a more robust, physical mobilisation soon led Chesser to seek out other opportunities, and his decision to attempt to join the Somali jihadist militia al-Shabaab appears to have been heavily influenced by ideas he had developed thanks in large part to Awlaki's online output (Brachman & Levine, 2011:36).

For radicalised Western Muslims like Chesser, supporting and preaching jihad online while remaining a resident in the West and doing nothing else to assist can come to be regarded as an unacceptable hypocrisy, making physical mobilisation an almost inevitable next step (Brachman & Levine, 2011:36). Chesser is therefore held up as an example of a person for whom the dissonance between his online persona and physical self became unbearable. Interesting too is that he failed in his attempts to find a real-world audience for his views, such as religious approval from local imams (USSCHSGA, 2012:20). As explained by Brachman and Levine, many global jihadists in the West whose contribution to the global movement amounts to high Internet activity (such as posting on jihadist forums or writing blogs in support of jihad and al-Qaeda), soon become aware of the vast discrepancy between their online and real-world physical

personas. The authors go on to argue that "online al-Qaeda supporters eventually want to become their avatar because it embodies all of the hopes, dreams, and goals that they are unable to actualize in the physical world" (Brachman & Levine, 2011:35). The creation of this online persona, then, can sometimes be the beginning of a process of radicalisation that can lead to physical mobilisation.

Thus, while there is little doubt that our understanding of the role of the Internet in the radicalisation process remains under-developed, recent years have seen an increased effort to address this through empirically based approaches. Most scholars are increasingly wary of making causal connections between an individual's involvement online and their mobilisation in the cause of violent ideologies and movements. It is therefore becoming increasingly rare to find literature that declares the Internet a cause of radicalisation, and emphasis is instead placed upon its facilitating and catalysing qualities. Nonetheless, scholars cannot ignore the cases that appear to go against the grain, and may have to re-assess this position if instances of so-called online 'self-radicalisation' increase.

Radicalisation vs. Recruitment

While much of the literature focuses on if and how individuals are radicalised online, many authors ignore the important distinction between radicalisation and recruitment. While, via the Internet, an individual may arguably go through a process of cognitive radicalisation – the adoption of the beliefs, and support for the actions, of an extremist movement – this will not necessarily lead to them mobilising or taking any actions on behalf of a group or movement. Neumann, for example, reminds us that, in the case of Irfan Raja, his entire radicalisation appears to have occurred online, but it was only after offline contact with four other like-minded individuals that he decided to go to Pakistan to receive training (Neumann et al, 2007:89).

Berger is also helpful here, and in a recent empirically grounded study reveals more specific details about online recruitment and how it takes place (Berger, 2015). In his study of the current ISIS recruitment strategy aimed at attracting Western foreign fighters – based on a database of approximately 1,600 Twitter accounts – he

found that during "first contact", ISIS recruiters make themselves available for interaction with sympathetic recruits while monitoring the activity of those they believe to have potential for recruitment, perhaps interacting through 'retweets' and 'favourites' as a way of showing acknowledgment (Berger, 2015:19–21). Once contact is made, recruiters will seek to create a micro-community in which the individual is bombarded with tweets while slowly being encouraged to isolate themselves from others, particularly those who follow more mainstream interpretations of Islam (Berger, 2015:21). Following this, the recruit is asked to transition on to private, encrypted messaging platforms such as Telegram where they are then encouraged to take action, often in the form of either terrorist attacks or making *hijrah* (migration) to the Levant (Berger, 2015:22).

Approaching a Consensus: the Least Contested Claims About the Role of the Internet

Despite disagreements in the field, there are a number of widely accepted advantages the Internet offers to extremist groups. Most obviously, the Internet provides the primary locus for individuals "to access radicalising material, instruction manuals and videos" (Weimann, 2014). In his explanation of violent extremist use of the Internet, Neumann explains that the Internet bandwidth now accommodating visual imagery (as opposed to text alone) and the rise of Web 2.0 has allowed extremists to access, and appeal to, a wider demographic. This includes those who are sympathetic and, perhaps more crucially, those who are not. This evolution from text-based propaganda to video, stated to be advantageous to extremists for its visually striking content (depicting beheadings and suicide attacks), is seen to have generated constant excitement and engaging debates (Neumann, 2012:17).

Other innovations in the range of materials now available digitally also include online magazines. For a time, al-Qaeda in the Arabian Peninsula's online magazine *Inspire* was unique in its targeting of Western audiences, specifically those vulnerable to the home-grown and lone-actor trajectory (Gold, 2012). Each edition has a section called 'Open Source Jihad', intended "to equip aspiring

jihadist attackers with the tools they need to conduct attacks without travelling to jihadist training camps" thus helping sympathisers in the West carry out attacks (Weimann, 2014; see also ADL, 2014). This has most recently been replicated by the ISIS-produced *Dabiq* and *Rumiyah* magazines, available in multiple languages and used to both legitimise their venture as well as call for attacks in the West (Gambhir, 2014). Numerous western jihadists have been found to have owned or read *Inspire*, including: Jose Pimental (arrested on suspicion of attacking returning US military personnel); Naser Jason Abdo (arrested on suspicion of planning a bomb attack at Fort Hood military base); Adel Daoud (arrested on suspicion of plotting a bomb attack on a Chicago bar in 2012); and Tamerlan and Dzhokhar Tsarnaev, the Boston bombers, who used the magazine's tips on using gunpowder extracted from fireworks as the basis for bomb-making (Weimann, 2014). However, a strong case for a causal connection between such materials, and violent acts perpetrated by those found to have been in possession of them, has yet to be made. Instead of making this connection, we must be willing to consider the possibility that seeking out and possessing extremist materials comes *after* an individual's initial radicalisation.

The combination of cheap production and editing tools and the freedom to disperse material provided by Web 2.0 explains the rise of so-called "Jihobbyists" who, despite being producers and consumers of material, do not have any direct or specific group affiliation (Brachman, 2009b; Neumann, 2012:17). Brachman states that, by designing their own propaganda, they are able to keep the extremist movement afloat and inflate the extremist narrative while simultaneously becoming more radicalised in the process (Brachman, 2009a). This helps us to understand why some of the online jihadist material depicts violent, gruesome action that is choreographed, well produced and is now available to watch across almost every possible platform (Weimann, 2014:13; Winter, 2015).

If an individual is immersed in this violent material for a significant period of time, it can result in desensitisation and 'mortality salience'. This refers to an acute awareness that one's own death is inevitable, thus theoretically making support for terrorist acts and

martyrdom more likely (Neumann, 2012:17–18; Abdollahi et al., 2006:527–536). For Winter, however, the crucial aspect of online propaganda is not that it necessarily causes individuals to join jihadist groups, nor carry out attacks at home, but that it can "catalyse the Islamist extremist's passage from tacit support to active member" (Winter, 2015:6).

However, while violence certainly features in jihadist propaganda, there are many other themes it covers that receive far less attention from the media and policy-makers. Milton, for example, points out that, in over 9,000 Islamic State visual media releases analysed for his study, "more than 50% focus on themes outside of the battlefield, such as governance, justice, the importance of religious practices, and life in the caliphate." Indeed, violence featured in only around 9% of the propaganda output sample (Milton, 2016:iv). In a related study, Winter found that, out of 892 "batches of propaganda" collected between July and August 2015, only 2.13% were focused on brutality, while 52.57% pushed the "utopia narrative" (Winter, 2015:21, 30). Findings such as these suggest that those who are influenced by extremist propaganda online are attracted to more than just violence, and this is reflected in extremist groups' efforts to present their activities in the context of a much wider mission to change, and improve, society.

It is also important to keep in mind that a great advantage of using the Internet comes from users' appetites to seek out and digest simplistic and reductionist answers to difficult, highly complex questions (Sageman 2004:162). In many respects, this is why Jihobbyists and other propagandists are seen to be so dangerous. Their ability to condense complex geo-political matters into a simplistic narrative makes them force multipliers and helps inspire those who go on to carry out attacks (Brachman, 2009b; Hussain & Saltman, 2014).

In conjunction with Jihobbyists, extremist movements also work to build a reputation for providing credible political news sources that offer a legitimate alternative to supposedly biased Western agencies that are seen as part of the conspiracy (Bergin et al., 2009; Hui, 2010; Kimmage, 2008a; Gold, 2012; Rogan & Stenersen, 2008). Their aim is to therefore emulate already established news outlets in the hope

of narrowing the credibility gap (Bergin et al., 2009:11). Such tactics aimed at increasing credibility include attempts to resemble objective reporting by distancing themselves from extremist movements by, for example, reporting about extremist organisations in the third person, and utilising English subtitles to demonstrate their international scope (Bergin et al., 2009:11). There is also evidence of efforts to replicate the production styles of leading Western media agencies (Maher et al., 2012:29). For Stevens, a crucial way in which the Internet facilitates radicalisation in conjunction with digital media is by allowing extremists to disseminate their narrative themselves without having to rely on journalists as middlemen, provided that they possess cheap and easily accessible equipment such as laptops and video cameras (Stevens, 2009:28; see also Betz, 2006:510).

Furthermore, the literature also refers to what are described as "authenticators" (Rogan & Stenersen, 2008; Hussain & Saltman, 2014; Kimmage, 2008a). These include, among other things, the use of specific logos and branding, and the targeted distribution, by language (Condon & Weyers, 2014), of media by a credible organisation in order to create an air of authenticity within a relatively sceptical community (Rogan & Stenersen, 2008). Kimmage documents how, within the online jihadist movement, there is also a great appetite for authenticity, not only to compete with Western media outlets as credible news sources, but also to maintain control over ideological content and direction (Kimmage, 2008a:5). The Islamic State's current media configuration is arguably the most complex of any non-state group in history, with five media foundations and 35 affiliates across the Levant, Maghreb and Sinai Peninsula (Winter, 2015:14). The ability of ISIS to create a "comprehensive brand" that retains a consistent visual aesthetic and message across its material has helped capture the imagination of recruits and potential sympathisers (Winter, 2015:6). Hussain and Saltman add to this by explaining in detail how issues of authenticity, and the emergence of "copycats", can confuse the followers of extremist movements (Hussain & Saltman, 2014:46). This, in turn, may begin to push extremists to gain their information from other followers on social networking sites.

ONLINE VS. OFFLINE INTERACTIONS

The majority of the literature takes a nuanced position that asserts the importance of online influences without negating the requirement of offline interactions. Some researchers stress that the impact of the real-world environment on an individual, and not just the influence of peers, is crucial in determining their vulnerability to turning to violence. Briggs, for example, argues that offline contacts are still a critical part of the radicalisation process (Briggs, 2011:3). However, she also concedes that, in the future, instances of individuals radicalising "entirely online" may increase (Briggs, 2011:3).

Theories that emphasise the appeal of being part of a close-knit group and the importance of physical networks in the radicalisation process also regard the concept of solitary Internet 'self-radicalisation' as unconvincing (Sageman, 2004:91; Durodie & Ng, 2008; Bergin et al., 2009; Chatham House, 2008; Pantucci, 2011; Hussain & Saltman, 2014; Hughes & Vidino, 2015). As we have already seen, Sageman highlights how interactivity between members online gives participants an opportunity to be swayed by the ideological content and begins to facilitate an "in-group love" (Sageman, 2004, 2008) that makes radicalisation more likely. Hoffman, meanwhile, places the onus on the importance of hierarchy within terrorist organisations, stating that 'official websites' and the ideological elite play the key role in facilitating individuals' radicalisation (be it through online or offline methods) (Hoffman, 2006).

Conway and McInerney support a synthesis of both positions. They suggest that Sageman's bottom-up theory explains the initial entry for youths seeking extremist content, while the Internet can enable the radicalisation of individuals with no prior connection to the movement by providing contact between them and extremists/would-be extremists online (Conway & McInerney, 2008:116). Hoffman's top-down approach then explains how terrorist organisations actively seek to connect with these vulnerable youth (Conway & McInerney, 2008:10).

In their study of American ISIS sympathisers and members on Twitter, Hughes and Vidino found that "purely web-driven"

radicalisation is undeniable. However, they also demonstrate that, in many cases, radicalised individuals "initially cultivated and later strengthened their interest in ISIS's narrative through face-to-face relationships". Like Conway and McInerney, they conclude that "online and offline dynamics complement one another" (Hughes & Vidino, 2015:ix).

Neumann takes the centrist view that the Internet radicalises because it provides a platform for like-minded individuals to build a network and potentially turn their terrorist aspirations into a reality. For terrorist recruiters, "it has also offered a pool of potential members that can be tapped into, with less risk than there would be involved in approaching an individual in the real world" (Neumann, 2012:19).

THE CREATION AND EVOLUTION OF THE 'JIHADISPHERE'

Within the online radicalisation literature, the Internet is seen as allowing for the creation of a virtual community for groups and movements that can support existing physical networks while disseminating different ideologies. In the case of violent extremists, this online milieu is often based in support of, or opposition to, an abstraction; in the case of global jihadism, an allegiance to the *ummah* (Mealer, 2012); in the case of the British far right, an alliance against what they regard as extremist Islam and the so-called 'Jewish conspiracy' (Goodwin, 2013; Bartlett & Littler, 2011). That these communities can exist is the result of the evolution of the Internet, a medium that has developed into an increasingly complex "data-exchange system" (Neumann & Stevens, 2009:10).

The phrase 'Web 2.0' is commonly cited in the literature and refers to the Internet's transition during the new millennium into a space encompassing "a growing array of interactive communications systems facilitated by a rapidly expanding set of platforms" (Amble, 2012:339). It gave birth to the platforms that we recognise today – "numerous websites, blogs, forums and message boards" (Ducol, 2012:51) – while laying the foundation for the most modern iterations of applications (or 'apps') and instant messaging services that have been seamlessly interwoven into the modern media landscape.

This evolution in the use of the Internet by jihadist groups led to the coining of the neologism 'Jihadisphere'. First used by Ducol, it is defined as a loose network of online communities that support the movement (2012:51–52). The individuals that are part of the Jihadisphere can be divided into three groups: passive members that tend to only consume online material (Ducol, 2012:58–59); producers of material that belong to various media arms of jihadist groups (Conway, 2012:5); and "Jihobbyists" (Neumann, 2013:435, Brachman, 2009a:19). Indeed, Brachman (who coined the term) describes these "Jihobbyists" as the backbone of the milieu. Likely aware that they are playing an important role, they feel empowered and more invested in the movement. For example, as a British far-right extremist interviewed by Behr et al. explained, his online activities "made him feel part of a group and important" (Behr et al., 2013:5). Combined with propaganda that encourages individuals to act in furtherance of their cause, violence becomes a distinct and very real possibility (Ramsay, 2009:34).

Static Websites

The online platforms upon which extremist groups rely to support their interactions have themselves evolved over time. The first of these platforms were official, or "top-down" websites (Zelin, 2013:5), created by ideologues and formal hierarchical groups as a way to communicate their goals and collective grievances on a cost-effective and uncensored global platform (Neumann, 2012:16). Others have also noted how this has allowed extremists to keep a memory of what a group has done by storing the documents produced as an archive or database (Della Porta & Mosca, 2009:777). Websites for extremist political parties tend to be the most rigidly hierarchical, unlike the more progressive alternative media in which a dialogue and a relationship is built between producer and consumer. In the case of the British National Party, Atton concludes that this rigidity has palpable real-world effects, for example, on supporters' ability to construct their own identities (Atton, 2006:573).

These websites aimed to better disseminate the ideology and facilitate contact through, for example, the posting of email addresses

(Rogan, 2006:17). The use of novel methods, particularly among the far right, transferred from the offline to the online world. Groups that once experimented offline with "fax-machines, 'dial-a-hate' hotlines, and AM radio programs" (Schafer, 2012:347), moved toward the creation of racist and violent video games once online. According to a study by Selepak the games required the player to violently kill, wound, and maim minorities in order to advance to the next level (Selepak, 2010).

Traditional (and often official) websites that have controversial or violent histories and exist within a hierarchical management structure are now in decline due to a combination of them being blocked or taken down, a growing paranoia among users that they were being monitored by government agencies and a general online shift to social media platforms (Hussain & Saltman, 2014:32; Zelin, 2013:5). This, in turn, has seen the rise of websites that produce a subtler narrative that slowly and more implicitly escalates in rhetoric, eventually pushing the user into more hard-line and extremist views (Hussain & Saltman, 2014:32; Bergin et al., 2009:7). In the context of far-right movements, often these narratives use fictional storytelling as a way of promoting their vision (Lee & Leets, 2002; McDonald, 1999). The power of storytelling lies in its ability to "make an argument without eliciting mental resistance" (Friedlander, 1992) which leads to fewer counter-arguments and less resistance to persuasion (Slater, 1990).

Extremist Forums

With the evolution of the Internet came the development of online forums that allowed members of extremist movements to bond with sympathisers and discuss political events, all in the relative security provided by online anonymity, and independent of large Internet companies (Neumann, 2012:16; Zelin, 2013:2). Given the scope these mediums provided for interaction, they soon began to outbid and replace static websites belonging to jihadist organisations as the main platforms from which to spread jihadist propaganda and create online networks (Ramsay, 2008; Zelin, 2013:5). Since many of these new platforms used English and Western languages other than Arabic, which had previously been the hegemonic language of jihadist

websites (Awan, 2007:76), jihadist content became more accessible to users worldwide (Ducol, 2012:52).

Despite this development, in Zelin's 2013 analysis of jihadist forums, he found that, in comparison to their Arabic counterparts, English language jihadist forums were far less active, suggesting that the movement was still heavily reliant upon the Arab world for its online activity. Nonetheless, Zelin's investigation, which is based on a quantitative analysis of three months' worth of selected jihadist forum activity, does uncover a significant reduction in major jihadist forums between 2009 and 2013 (Zelin, 2013:2). He attributes this to a number of factors, including an increase in the use of social media and government takedowns of popular forums. The 'hey-day' in jihadist forum usage, meanwhile, was in the mid-2000s, which Zelin partially puts down to an increased desire to open up the online jihadist communication infrastructure to a wider audience. Whereas previous jihadist online activism was limited to top-down official al-Qaeda websites, these new forums "shattered the elitist nature of *jihadi* communications" (Zelin, 2013:5). A number of scholars credit the work of leading global jihad strategist Abu Mus'ab al-Suri in spearheading this change (Lia, 2009; Brachman, 2009a; Zelin, 2013).

Such forums are particularly useful for extremist propagators because of their anonymity. This can facilitate greater feelings of connection (Sageman, 2004), while providing those who would "never normally engage in criminal or risky behaviour in the physical world" the ability to "confide in the safety of their surrounding online environment" (McFarlane, 2013:5). This anonymity is thought to help put individuals at ease when asking questions about taboo subjects (e.g. sex, relationships, etc.) and also grants greater authority to users posing as ideological experts on what to do, be it bomb-making or issues of integration (Bunt, 2003; Weimann, 2010; Bergin et al., 2009; NCTb, 2010a; Singh, 2009). While probably a feature of the Internet as a whole, this dynamic is most powerful on platforms such as online discussion forums as people are more reluctant to act out on their personally identifiable accounts (Bakker & Hille, 2014:563). Anonymity creates an "online disinhibition" effect that, in its "toxic" form (Suler 2005), gives people a sense of security in avoiding responsibility for

their virtual pronouncements, but which may have the consequence of such groups becoming more hostile, polarised and potentially prone to violence (Koehler, 2014:118). In his work with former German far-right extremists, Koehler identified anonymity as the second most common attribute among the interviewees (after cost, accessibility and efficiency of communication) as it provoked individuals to speak or act out more online than they normally would offline (Koehler, 2014).

The Shift to Social Media

While chat rooms and forums have become less reliant on password protection (Weimann, 2010), in the current environment, extremists are looking more towards free-to-access and public social media platforms to propagate their messages and recruit people (Weimann, 2015). In Zelin's 2013 analysis he predicted that, despite the increased use of social media by jihadists, the centre of gravity for their online operations would remain the forums that ostensibly allow jihadists "the ability to have relatively private conversations" (Zelin, 2013:1). However, developments in the use of platforms such as YouTube, Twitter, Instagram and Telegram among Westerners joining jihadist groups in Syria (for more, see Carter et al., 2014; Bradford et al., 2015) suggest that, while an understandable conclusion at the time, it was somewhat premature. This use of social media has made online jihadist activism far more accessible to the general public. It also means that the traditional relationship between mainstream media and violent actors has been somewhat reversed – with the former now relying more on the latter's social media output for information gathering and non-state violent actors no longer requiring the mainstream media to disseminate information as they once did (Klausen, 2015:6).

In the current environment, extremists are looking more towards free-to-access and public social media platforms to propagate their messages and recruit people.

Some authors have gone as far as suggesting the possibility that online social networks can have the same or a similar effect upon radicalisation and mobilisation as physical milieus and face-to-face

interactions considered so central to this phenomenon (Briggs, 2011; Conway, 2012; Pearson, 2015). Bjelopera goes further, claiming that the level of readership and authorship interactivity now available to jihadist groups has helped to encourage people who interact online "to more easily see themselves as part of broader jihadist movements and not just casual readers or online spectators" (Bjelopera, 2013:20–21).

In her exploratory study on this issue, Conway also investigates whether, with the advent of Web 2.0, the Internet now shares more characteristics with traditional radical milieus and asks if indeed it can have the same kinds of effects as more formal, face-to-face socialisation processes (Conway, 2012:4). To this end, in her study of female participation in online extremist networks and the role it plays in their radicalisation, Pearson highlights the creation of an "online sisterhood" of female ISIS supporters. This network allows its members to interact about numerous topics, including travel to Syria, and offers support structures for members who have lost husbands fighting for ISIS (Pearson, 2015:17). Accordingly, "such messaging supports the gender ideology of the Jihad" (Pearson, 2015:17). Behr et al. share this conclusion; in their qualitative study, online interactions were considered to be, if not a direct cause, then certainly a facilitator of radicalisation. It also leads to an escalation in extremist sentiments, as violent extremists intensify their statements in order to comply with or appease other members' views (Geeraerts, 2012).

Both Koehler and Wojcieszak find that this is as true for neo-Nazis as it is for jihadists, with Koehler arguing that extremist use of social media creates the perception of a critical mass within the movement that motivates individuals to get further involved and possibly carry out more extreme actions (Koehler, 2014:121). This then reflects the group dynamics that Sageman identified in the real world, where opinions gradually become more extreme as members of the groups become more insular and exclusively reliant on the group for social interaction (Wojcieszak, 2010:10–11; Sageman, 2008:87). As Conway and others concede, while the assertion that online networks can have the same impact as physical ones is yet to be proven, it remains an interesting and fruitful avenue for future research.

Social networking sites are seen to offer a significant advantage due to the ease with which one can create a new account and the relative safety they provide from being tracked through an Internet Protocol (IP) address (Behr et al., 2013:34). Furthermore, these social networking sites have maximised accessibility; whether sympathetic or not, anyone can fall foul of online material that no longer exists in the periphery of the "darkest corners of the Internet" (Neumann, 2012:17). This has coincided with an increase in the number of languages that jihadist propaganda is now published in (Bermingham, 2009; Condon & Weyers, 2014), as well as allowing engagement with new demographics, most notably women (NCTb, 2010a; Malik & Rafiq, 2015; Pearson, 2015; Saltman & Smith, 2015).

Weimann tells us how Facebook is especially important for "letting terrorists find mainstream Islamic youth who may on occasion view jihadist content and link them to the more… hard-core sympathisers" (Weimann, 2014:67), or a "gateway" to extremist sites and operational information (DHS, 2010). Twitter, meanwhile has become "the main hub for the active dissemination of links directing users to digital content hosted on a range of other platforms" (Fisher & Prucha, 2013:21), while YouTube has fostered a "thriving subculture which uses it to communicate, share propaganda, and recruit new individuals" (Weimann, 2014:10). Weimann highlights the development of comments sections below videos as a crucial step, noting that "(t)he ability to exchange comments about videos and to send private messages to other users help *jihadists* identify each other rapidly, resulting in a vibrant *jihadist* virtual community" (Weimann, 2014:10). Instagram and Flickr have also been "littered with radical propaganda glorifying terrorist masterminds such as Osama Bin Laden and Anwar al-Awlaki" (Weimann, 2014:13). Western countries, in particular the US, protect the freedom of user-generated content, causing extremist propagators to flock to these areas (CHSHR, 2007).

Social media has provided a level of accessibility that allows individuals to selectively surround or implant themselves into communities and milieus of like-minded individuals, connected via different platforms (Carvalho, 2014). The process and product have been described differently in the literature, from "echo

Twitter, by its very nature, is particularly conducive to the creation of echo chambers. It allows for narrow environments to be cultivated around users which ensure that information appearing on their feed is tailored to their specific interests and beliefs, often to the detriment of divergent views and dissenting or alternative opinions.

chambers" (Neumann, 2012; Geeraerts, 2012; O'Hara & Stevens, 2015; Hughes & Vidino, 2015) to "cyberbalkanisation" (Alstyne & Brynjolfsson, 1997:3). Many studies argue that such echo chambers allow for the unchallenged support and amplification of the most extreme views in a community (Briggs, 2011:6; Bjelopera, 2013:18). This also leads to fewer dissenting voices and helps users embrace extreme ideas: "As a result, people acquire a skewed sense of reality so that extremist attitudes and violence are no longer taboos but – rather – are seen as positive and desirable" (Neumann, 2012:18). Twitter, by its very nature, is particularly conducive to the creation of echo chambers. It allows for narrow environments to be cultivated around users which ensure that information appearing on their feed is tailored to their specific interests and beliefs, often to the detriment of divergent views and dissenting or alternative opinions.

Among the most recent developments in the terrorist threat made possible by a combination of social media and encrypted messaging apps is the emergence of "virtual plotters" (Callimachi, 2017; Amarasingam, 2016; Moreng, 2016; Prucha, 2016). In one of the most in-depth studies to date on the use of Telegram by ISIS, Prucha argues that it has not only become "the most important information outlet" for the group, but that it "has been used to recruit and guide attackers in Europe" (Prucha, 2016). A number of ISIS-inspired attacks in America, Europe and South Asia, which were initially assumed to be the work of lone actors, were later found to have been coordinated and directed over the Internet by ISIS members residing in the group's territories in Iraq and Afghanistan. One study on ISIS-linked terrorism in Europe has found that, out of 38 total plots between 2014 and October 2016, 19 were found to have involved "online instruction

from members of IS's networks" (Nesser et al., 2016). One of the most effective virtual plotters thus far has been Rachid Kassim who, using his encrypted Telegram channel, contacted willing ISIS recruits in France and gave them operational guidance, helping to focus and hone their desire to carry out a terrorist attack in their home country (Amarasingam, 2016). Investigators have linked him to a number of attacks in France, including that of Adel Kermiche and Abdel Malik Petitjean, who, in July 2016, killed Catholic priest Jacques Hamel as he presided over morning Mass in his church in Normandy. Jean Charles Brisard of the Centre for the Analysis of Terrorism in Paris has also claimed that Kassim guided over half of the 17 foiled jihadist plots in France in 2016 (Browne & Cruickshank, 2017). Kassim is thought to have been killed by a US air strike in February 2017.

In a similar fashion, a group dubbed by the FBI as "the Legion", based in Raqqa and originally headed up by a young British hacker named Junaid Hussain, has directed at least four different plots and attempted attacks in the US (Goldman & Schmitt, 2016). One of the American terrorism cases linked to Junaid is that of American Ohio resident Munir Abdulkader, who, in July 2016, pleaded guilty to attempting to murder government employees and officials, possessing a firearm and attempting to provide material support to ISIS. In court documents relating to his trial, it is claimed that Abdulkader "was in electronic communication with at least one member of ISIL overseas named Junaid Hussain, and placed himself under the direction of ISIL and its overseas leadership" (USA vs. Munir Abdulkader, 2016:3). In their communications, Hussain had "ultimately laid out… an overall terrorist attack plan for Abdulkader… to implement" (USA vs. Munir Abdulkader, 2016:10). More specifically, Hussain had instructed Abdulkader to kidnap an American soldier and record his killing on camera, and then suggested that he attack a police station in Cincinnati. Hussain was deemed such a threat to Western security interests that he was targeted and killed by a suspected drone strike in August 2015.

The advent of virtual plotters represents an evolution of jihadist terrorist tactics that was made possible by the rise of social media and likely marks a trend that will define much of the threat picture

in the West in the near future. As ISIS continues to lose ground in both Iraq and Syria, it will increasingly rely on the ability of such figures to reach out to supporters abroad in order to maintain the group's presence and ability to strike against its enemies. This will present both Western governments and technology companies with new and complex challenges, and may increase the pressure on both to find effective solutions.

SOCIAL MEDIA: A NEW SOURCE OF EMPIRICAL DATA

The use of social media by extremists has also opened up new avenues of research, allowing for access to the sort of empirical data that is notoriously difficult to come by when studying radicalisation and terrorism. The foreign-fighter phenomenon in Syria and Iraq has, to date, provided among the richest datasets of extremists using the Internet, with studies utilising information and data drawn from Western Twitter users based within Syrian jihadist groups (Carter et al., 2014; Bradford et al., 2015; Saltman & Smith, 2015; Berger, 2015; Hughes & Vidino, 2015; Pearson, 2015).

Drawing from among the largest databases of Twitter accounts used by European ISIS members, Carter et al. note how effective social networking sites have become in helping to establish virtual networks through which "a large number of foreign fighters receive their information about the conflict not from the official channels provided by their fighting group but through so-called disseminators" (Carter et al., 2014:1). These disseminators are described as being sympathetic individuals who are able to contribute violent extremist narratives from the comfort and relative safety of their Western homes. They provide live updates from far-away battles, quickly becoming major (and also trusted) sources of conflict information for foreign fighters (Carter et al., 2014). In a similar study, Klausen's findings partly corroborate these conclusions, but she argues that other, lesser known social media users have been more impactful than those identified by Carter et al. (Klausen, 2015:14).

"Disseminators" are not classified as foreign fighters and have no official links to any jihadist organisations. Instead, these

individuals "broadly support the Islamist project in Syria" providing "moral and political support to the cause" (Carter et al., 2014:15). The influence of sympathetic individuals, the "Jihobbyists" referred to above, is epitomised by the example of Younis Tsouli. Carter et al., argue that, just as online jihadist forums facilitated Tsouli's propagation of extremist materials, Twitter has allowed the role of disseminators to evolve even further (Carter et al., 2015:15–16). Among other advantages, Twitter gives disseminators of extremist material a platform from which to engage with their followers rather than the one-way communication coming from official accounts (Carter et al., 2014:18). Spiritual leaders, which many extremists have either turned to for justification (Bunt, 2003), or have been manipulated by (Bhatt & Silber, 2007), are also evolving through the use of social networking sites. Facebook has facilitated the creation of many of these leaders in allowing for the establishment of personal profiles and fan pages that enable users to interact and seek justification for their beliefs and actions (Carter et al., 2014).

In the American context, the most comprehensive analysis of ISIS Twitter users' activities is provided by Hughes and Vidino. In their study, they offer three of the key manifestations of ISIS use of Twitter to reach its audience in the West: "1) triggering or advancing their radicalization process; 2) helping them mobilize to leave for Syria to join the group; and 3) inciting them to carry out attacks in America." (Hughes & Vidino, 2015:19). Referring to the ISIS Twitter world as an "informal echo chamber", they describe how their sample of 300 American ISIS Twitter users performed three distinct roles: "nodes" are those accounts which generate new content; "amplifiers" retweet pro-ISIS materials; and "shout-outs" help to promote new accounts set up by previously suspended users (Hughes & Vidino, 2015:24–25).

It was also pointed out that a third of the users within the sample described themselves as female. While it should not be seen as an entirely separate phenomenon, the radicalisation of women and the role played by their involvement on social media has been in the spotlight recently due, in part, to the growing trend of females travelling to Syria and Iraq to live under ISIS. As a result, a number

The Internet (social media in particular) and the array of advantages it offers extremist groups remains one of the biggest challenges facing counter-terrorism and law enforcement authorities.

of recent works have specifically focused on the radicalisation of women and their online activities in support of the group. (Bloom, 2013; Bradford et al., 2015; Pearson, 2015; Saltman & Smith, 2015).

Modern social media platforms have been crucial in facilitating a means to continue this phenomenon, allowing women to communicate and network with other extremists virtually, which can have significant import given the frequent lack of opportunities for females to be fully integrated in 'real world' settings (Sanchez, 2014; Bermingham et al., 2009; Carvalho 2014). Within the global jihad movement, a new generation of leaders look to women to help "ensure the survival of the organization by devising new religious justifications that would allow women to participate in violent *jihadist* activities" (Bloom, 2013:150). The Internet has equalised and democratised gender roles within groups, affording women "the opportunity to manipulate cultural gender norms as well as to disguise their gender while participating in traditionally male-sanctioned *jihadi* activities" (Bloom, 2013:156; see also Conway, 2017:89–91).

The Internet (social media in particular) and the array of advantages it offers extremist groups remains one of the biggest challenges facing counter-terrorism and law enforcement authorities. Not only is research on this topic still in its nascent stages and unable to offer any concrete understandings, the issue has also led to increased tensions between technology companies and states. One of the key challenges will be how liberal nations and the companies that operate within them maintain their commitments to free speech and expression, while also devising ways to counter this fluid and evolving threat. The following section will delve deeper into the nature of the challenge of countering online radicalisation and what policies have begun to take shape around the world.


COUNTERING
ONLINE
RADICALISATION

GIVEN THAT THE debate surrounding countering violent extremism exists in the nexus between security and civil liberties, it is an understandably complicated and emotive issue. This section will categorise such policies and recommendations in three ways: 'hard approaches' refer to government measures that are necessarily intrusive, and involve the restriction of Internet content for security purposes; 'soft approaches' refer to measures with limited intrusion, focusing instead on the importance of building so-called counter-narratives and empowering online actors to engage and denounce extremist propagators; while 'intelligence-led' approaches bleed into both hard and soft tactics, and are centred on the function of intelligence gathering and monitoring. There exists a high degree of overlap between these approaches and they should not be treated as homogenous blocks.

Most Western government efforts to respond to online radicalisation fall under the umbrella of what is commonly referred to as Countering Violent Extremism (CVE). CVE policies and initiatives are usually aimed at either countering radicalisation of various ideological stripes by attempting to prevent individuals from adopting extreme ideas and actions, or de-radicalising those who have already gone further down the path. It is a term that has, at times, courted controversy. A number of Western Muslim organisations see it as a cover for government efforts to unfairly victimise and attack Muslims (CAIR, 2015). At the opposing end, many have criticised CVE as far too general in its approach, failing to go far enough in focusing specifically on jihadist terrorism. Indeed, it may be that the latter position characterises the thinking of the new American administration under President Donald Trump, with as yet unconfirmed reports suggesting that the US Government's existing CVE programme will be renamed 'Countering Islamic Extremism' or 'Countering Radical Islam' (Ainsley, Volz & Cooke, 2017).

HARD APPROACHES AND NEGATIVE MEASURES

Hard approaches (also referred to as negative measures) largely revolve around "technical solutions" (Neumann & Stevens, 2009:1) such as the denial and/or removal of extremist content on the Internet.

The logic here is that by restricting extreme material, fewer individuals will be radicalised. A number of options are available for this approach, including: removing (instructing the host website to take the content down); filtering (controlling the information between computers that are connected through the Internet via Internet Service Providers (ISPs)); and hiding (interfering with search engines so as to ensure that extremist-related websites appear near the bottom and are thus less visible) (Neumann & Stevens, 2009).

Proponents of hard approaches also state that online freedom in the West provides safe havens for extremist propagators to extend their message, thus justifying stronger measures (CHSHR, 2007:4). Writing in the *New York Times,* Martin London notes a legal hypocrisy within existing Western laws that allows for extremist material to be promulgated openly as they are protected under constitutional freedoms. Without specifically condoning this, he points out that other material, such as child pornography, does not enjoy the same extent of legal protection (London, 2015). More controversially, the then British Prime Minister, David Cameron, emphasised the need for social networking communication sites to better cooperate with government intelligence services, a heretical move in the eyes of Internet privacy campaigners (Griffin, 2015).

Such cooperation, however, does not have to be inherently clandestine or pernicious. Park and Suyin draw our attention to a memorandum of understanding between the Swiss authorities and eBay authored in a bid to combat illicit trafficking of cultural property through the Internet (Park & Suyin, 2010:2). Finally, Rogan and Stenersen's analysis, revolving around the use of the Internet as a "virtual training camp for *Jihadists*", also advocates a policy approach that pressures ISPs to heed the moral duty of removing extremist sites from their servers (Rogan & Stenersen, 2008:6).

Among the first efforts to create a coordinated response to extremist use of the Internet was EUROPOL's creation of the 'Check the Web' project in 2007, which seeks to provide a mechanism for EU member states to "share information on Islamist terrorist activities on the Internet via the secure EUROPOL network and the EUROPOL national units". Among other things, it serves as a digital reference library of

primary online jihadist propaganda. In establishing this, EUROPOL aims to "create synergies between the Member States in the analysis of online Islamist terrorist activities" (EUROPOL, 2013:57).

This was then followed up in July 2015 with the introduction of the EU Internet Referral Unit (EUIRU) with the stated aim of combating "terrorist propaganda and related violent extremist activities on the Internet" (EUROPOL, 2015). It planned to approach the problem by serving as a central hub for relevant partners in EU states that would coordinate the identification, referral and flagging of violent extremist content on the Internet and work to develop efficient ways to respond. Its primary tactic involves working with online service providers in order to ensure the removal of flagged extremist content online.

In July 2016, the EUIRU released a report detailing statistics related to its achievements in the year since its establishment (EUROPOL, 2016). Among the more notable figures is that by 1 July 2016, 8,949 separate pieces of jihadist content were removed, compared to just 511 in the previous year. In addition, it had added a total of 13,298 separate primary jihadist materials to the Check the Web library (EUROPOL, 2016:7–11). The annual report also explains how the EUIRU had taken on an operational support role by "supporting Member States with Internet investigation activities." Since this expansion in its remit, the EUIRU has provided this support to 44 operational cases related to jihadist terrorism in Europe (EUROPOL, 2016:6).

The British Government is among those that have included similarly hard approaches as part of a strategy for combating violent extremist use of the Internet. In 2010, the Association of Chief Police Officers launched the Counter Terrorism Internet Referral Unit (CTIRU), which is intended to be part of an effort to make the Internet "a more hostile place for terrorists" (Hertfordshire Police). It is therefore responsible for identifying and tracking individuals who disseminate terrorist propaganda and helps the authorities in their efforts to persuade Internet companies to remove or block offending websites, social media accounts and materials (UK Home Affairs Committee, 2016:4; Edwards & Gribbon, 2013:46).

A number of major Internet companies have also begun to take a more proactive role in this realm and are aggressively identifying and

removing extremist users and content from their platforms. In early 2016, Twitter announced that it had suspended 125,000 accounts "for threatening or promoting terrorist acts". The company also announced that it had increased the size of its teams which identify extremist content to ensure a reduction in response times (Twitter, 2016).

Within the literature, advocacy for the hard approach is, however, in the minority. Most work on this topic regards such measures as impractical at best and dangerous at worst (Brown, 2010; Brown & Cowls, 2015). Brown and Cowls, in their study on the ethics and politics of policing extremist material online, warn that such approaches must be proportional to the threat, lest they begin to infringe upon civil liberties:

> Interferences must be necessary to achieve a legitimate aim, and proportionate to the aim – more significant reductions in harm might justify more significant interferences, but assessments must also take into account potential societal harms from interferences with rights (Brown & Cowls, 2015:11).

They also stress the importance of an inclusive counter-terrorism process, which allows the public to play a role in community security and intelligence, quoting Bartlett et al. to emphasise the point: "Serious and recognised damage to security occurs when the state's efforts are not accepted or trusted" (Bartlett et al., 2012:18). Indeed, it appears that British authorities have heeded such suggestions, with the CTIRU creating a dedicated website page allowing for public reporting on content they encounter online they deem to be in breach of counter-terrorism legislation (Walker & Conway, 2015:166).

Another commonly identified problem involves basic legal practicalities. The transnational nature of this phenomenon – whereby one country can host a website that incites violence in another, while the extremists behind it plan operations in a third country – would require equally transnational cooperation in order to implement these negative approaches (Bergin et al., 2009). While the efforts of EUROPOL certainly represent an attempt to address the lack of cross-border cooperation, the global nature of the Internet

How best to conceptualise, and therefore respond to, modern extremist groups' propaganda dissemination strategies remains a point of debate within the literature.

makes "common action to take down websites … legally irrelevant in the absence of a binding international treaty and consensus on what material should be subject to censorship" (Bergin et al., 2009:15). In other words, policing the whole Internet is not only impractical, but also undemocratic (Ryan, 2007:86–88; Brown & Cowls, 2015). Such online footprints also provide an invaluable source of intelligence. The platforms and mediums that allow for pernicious communications (that are increasingly occurring over open platforms) provide a wealth of information and materials for authorities and researchers alike (Yasin, 2011:2; Edwards & Gribbon, 2013).

How best to conceptualise, and therefore respond to, modern extremist groups' propaganda dissemination strategies remains a point of debate within the literature. Winter has found that the dissemination of information is now outsourced and decentralised: "disseminators are, most of the time, self-appointed and have no official position in the organisation, virtual or otherwise" (Winter 2015:7). Klausen supports this to a degree, noting that "the new lateral social media environment control over content is *decentralized*. Anyone can participate" (Klausen, 2015:3). However, behind the apparent spontaneous activity, the production "is managed more tightly than is generally recognized … communications of the fighters are restricted and only trusted militants maintain high volume social media activities" (Klausen, 2015:2).

Regardless of this ambiguity, the resultant effect makes the new media environment "resistant to policing" (Klausen, 2015:2) leaving groups such as ISIS insulated from government-led schemes to censor its content (Winter, 2015:7). The nature of social media platforms, combined with the saturation of the virtual space with extremist material, means that profiles can reappear within a short space of time after being taken down (Hussain & Saltman, 2014; Berger & Morgan, 2015). Diplomatic tension is also a genuine concern, and Western governments' bullheadedness in approaching

negative measures undoubtedly has the capacity to strain relations with other countries and organisations (Neumann & Stevens, 2009; Hussain & Saltman, 2014; Bergin et al., 2009).

Berger and Perez, however, have pushed back against claims that hard measures are ineffective. In a 2016 empirical network analysis study of approximately one thousand English-speaking ISIS adherents on Twitter, they found that account suspensions had the effect of "devastating the reach" of important and influential users (Berger & Perez, 2016:4). The impact of such measures on users who started new accounts after being repeatedly suspended, for example, was found to diminish with each new account created. Suspensions also led to a reduction in the amount of ISIS material available online, as they were usually followed by a deletion of all tweets by suspended users (Berger & Perez, 2016:4). The suspension of user accounts by Twitter is based on a violation of pre-agreed terms of service. Arguably, this does not amount to undemocratic censorship of the type Brown and Cowls warn against, especially when it relates to the suspension of accounts that make direct calls for murder or terrorism. The process which Twitter goes through to determine if a user is violating its terms of service, however, remains unclear.

Internet companies, governments, and researchers alike are still faced with problems associated with negative measures. What constitutes extreme material? What should be censored? The proven effectiveness of negative measures used to filter and remove child pornography, for example, is not easily transferrable due to the ambiguity that surrounds the definition of extremist material, as opposed to the former which has a clear definition and guidelines (Neumann & Stevens, 2009; Hussain & Saltman, 2014; Bergin et al., 2009). The problem with deciding what is and is not extreme is further exacerbated by filtering measures because they have been proven to also filter legitimate websites and material (Neumann & Stevens, 2009; Hussain & Saltman, 2014; Neumann, 2012). Furthermore, any attempt at effective filtering, hiding and removing will require a large amount of financial resources and would likely impact on high-speed Internet connections (Neumann & Stevens, 2009).

Related to this, Russell and Saltman also warn that a focus simply on 'violent extremism', as opposed to extremism more generally, has had a detrimental effect on counter-extremism policies such as the UK's Prevent strategy. Thus, such strategies "should focus on the causes of... violence, and therefore address the ideological roots of extremism of all kinds, whether violent or non-violent" (Russell & Saltman, 2014:3). While they agree that the law should be enforced against hate speech and illegal extremist material, the nature of the threat also means that such policies must also "focus on a strategy that centres on civil society action, engagement with extremist ideologies and narratives, development and dissemination of counter-narratives, and addressing the grievances perceived by those vulnerable to ... radicalisation" (Russell & Saltman, 2014:3).

SOFT APPROACHES AND COUNTER-NARRATIVES

This brings us to works that prescribe soft approaches which are based on the assumption that intrusive measures are detrimental to the cause of countering online radicalisation. It is hoped that countering the narrative online will begin to put pressure on the supply, rather than producing the 'whack-a-mole' effect (whereby censored material quickly turns up somewhere else on the Internet) that is sometimes but not always, as Berger and Perez remind us, apparent within the hard approach of suspending accounts. Soft approaches emphasise educating moderate or mainstream online users and communities on the dangers of extremist material on the web. By creating greater awareness of the extremist material, and greater awareness of the mechanisms they can use to report such materials, some believe that a self-regulated Internet will gradually take shape (Bergin et al., 2009; Neumann & Stevens, 2009; Ali, 2008; Ashour, 2010; Durodie & Ng, 2008; Briggs, 2011; Hussain & Saltman, 2014).

This is a user-driven answer to an increasingly user-driven problem and includes the strategy of improving 'media literacy', a term defined by the UK communications regulator Ofcom as "the ability to access, understand and create communications in a variety of contexts" (Ofcom, 2006:3). Increasing the media literacy of Internet users

will leave them more sensitive to extremist material, and thus more effective in reporting and engaging with it. Those who advocate this position also give suggestions on who should play a role in improving the media literacy of the community, including schoolteachers, parents and government (Neumann & Stevens, 2009; Ryan, 2007). Training to protect users from online extremists would mimic the training individuals already received to protect themselves from sexual predators (White House, 2011:6). However, although government is cited as a 'stakeholder', soft approach advocates emphasise caution on the level of governmental input (Neumann & Stevens, 2009; Hussain & Saltman, 2014; Aly et al., 2014; Klausen, 2015). Hussain and Saltman, for example, stress that "countering online extremism must be a joint effort between governments, civil society and the private sector" (Hussain & Saltman, 2014:107). Aly et al. echo this claim, arguing that the "credibility of the source is a decisive factor for ensuring the persuasiveness of any communication" (Aly et al., 2014:43). Once the source is considered credible, it is argued that partners from within the targeted community must also be involved in order to retain legitimacy (Aly et al., 2014:44).

A number of such approaches have been implemented by states since the September 11, 2001 attacks on New York and Washington, D.C. In 2007, the British Government established the Research Information and Communications Unit (RICU) within the Office for Security and Counter-Terrorism (OSCT) and gave its staff a brief to develop effective anti-extremism communications strategies over a range of platforms. As a unit run jointly by the Home Office, Foreign and Commonwealth Office and the Department for Communities and Local Government, it represents one of "the most developed cross-departmental strategic communications units in Europe" (ISD, 2013).

In the US, among the first efforts to contest an online space seemingly dominated by extremists was the US State Department's Center for Strategic Counterterrorism Communications' (CSCC) 'Think Again Turn Away' counter-narrative social media campaign (Walker & Conway, 2015:168). Established in late 2013, it operated largely as a Twitter feed which provided counter-messaging material aimed at delegitimising the ISIS message. In addition, it directly

engaged with jihadist users, attacking them and attempting to expose the hypocrisies within their ideology.

However, the approach was met with fierce criticism that variously included its inferior production quality which left its output looking amateurish in comparison to that of ISIS, having unedifying and counterproductive Twitter battles, and helping to amplify the voices of those it attacked (Katz, 2014; Atran & Hamid, 2015). The project has since been discontinued, and the State Department has replaced it with the Global Engagement Center. Its stated aim is to "more effectively coordinate, integrate and synchronize messaging to foreign audiences that undermines the disinformation espoused by violent extremist groups, including ISIL and al-Qaeda, and that offers positive alternatives" (US State Department, 2016). Among the departures from its previous efforts is that the State Department envisages this as a more 'hands-off' approach, which empowers others and avoids directly engaging online.

In Europe, the EU established the Radicalisation Awareness Network Internet and Social Media Working Group (RAN@) in 2012 under the Directorate General Home Affairs. Its primary focus is research into online radicalisation and counter-messaging with the goal of developing "frontline partnerships around the collation, creation, and dissemination of counter- and alternative-narratives through the Internet and social media" (RAN, 2012; Walker & Conway:169). The group has also made an effort to define counter-narratives, describing them as those which "directly or indirectly challenge extremist narratives either through ideology, logic, fact or humour" (RAN, 2012a:1). It also seeks to differentiate counter-narratives from what it describes as "alternative narratives", which "counter radicalization towards violence by putting forward a positive story about social values, such as tolerance, openness, freedom and democracy" (RAN, 2012a:1).

Further afield, the Sakinah project in Saudi Arabia is often cited as an example of an initiative that the Saudi Government has "quietly supported" to combat Internet radicalisation (Boucek, 2008:1; Janbek & Seib, 2012:107). It uses the tactics of extremists (as described above by Berger, 2015) to engage with those that seek religious knowledge using the Internet. Having engaged them on an open platform,

the Sakinah operative will suggest moving to a private platform, and involve them in conversations that steer discussion towards moderate interpretations of scripture while demonstrating fallacies in the arguments of extremists (Boucek, 2008:2).

The private sector has also taken on the challenge of confronting extremist messages online. One of the biggest and most well-resourced efforts comes in the form of Alphabet's 'Jigsaw' initiative. Alphabet, the parent company of Google, set up Jigsaw in order to build technology designed to "tackle some of the toughest global security challenges facing the world today – from thwarting online censorship to mitigating the threats from digital attacks to countering violent extremism" (Jigsaw, 2016). It also provides funding to Internet-related projects that help progress its aims. Among these is 'Abdullah-X', an initiative run by a former extremist who creates online animated shorts that offer "critical, thought provoking and engaging online content backed by offline engagement" and reject extremist interpretations of Islam (Abdullah-X, 2016).

Jigsaw also helped to set up the 'Redirect Method', a practical approach that arguably offers more tangible benefits than counter-messaging alone. This uses Adwords, an online advertising algorithm, to target people who are "actively looking for extremist content and connections" (Jigsaw, 2016). The focus here is not on the creation of any sort of new content, but rather on "divert[ing] young people off the path to extremism using pre-existing YouTube content and targeted advertising" (Jigsaw, 2016). This first involved a process of interviewing ISIS defectors, mapping the key ISIS narratives that drive radicalisation and recruitment, and identifying existing online content (in English and Arabic) that offers different views of the world, some of which was not specifically designed to counter ISIS.

Using this base knowledge and content, the Redirect Method developed a "targeting framework" using Adwords to identify Internet users who were searching keywords that suggested they had a positive view of ISIS (The Redirect Method, 2016). These users would then become the targets of ad campaigns based on the pre-identified anti-ISIS online content. According to its website, over an eight-week pilot period the Redirect Method reached 320,906 people, who watched 500,070

minutes of video linked to the ad campaign (The Redirect Method, 2016). While it remains difficult to determine who precisely this campaign reached, this method appears to be the most effective way of ensuring that counter-narrative content reaches its intended audience.

Among the benefits it offers, the soft-approach strategy protects against Internet censorship, a strategically advantageous step in the security versus liberty debate. Kimmage argues that Web 2.0 should not provoke censorship, but should be exploited as a tool to counter online radicalisation. He points to examples where al-Qaeda videos on YouTube are criticised in the comments section, a system which allows for the praise the material often receives within the online extremist milieus to be challenged. This therefore represents a significant change from the often uncontested platforms within traditional Web 1.0 channels (Kimmage, 2008b; Neumann, 2012). The diffuse nature of Web 2.0 then arguably creates new vulnerabilities for extremist ideologies, as it puts them squarely in the centre of online communities and users who, on the whole, reject the extremist content while engaging with it.

In addition to user backlash, jihadist groups also seem increasingly aware of the lack of command over ideological material on Web 2.0, and this again is demonstrative proof for soft approach advocates of the virtue of an unrestricted Internet as a tool against extremism (Kimmage, 2008b). Sageman explains how the leaderless jihad movement has resulted in more dynamic ideologies that shift in their particular context, meaning that the movement is vulnerable to self-implosion if governments successfully pursue soft approaches to countering radicalisation. For him, Western foreign policy is becoming less intrusive, and jihad and extremist ideology have become more violent. Thus, if allowed to fester in an uncensored Internet, the narrative will become less appealing (Sageman, 2009).

Scholars have also made much of online cleavages among the extremist propagators themselves, which may be exploited to compromise the utility of the Internet for extremist movements. Both Weimann and Conway separately highlight some of the contested issues between jihadists and other Islamists and their sympathisers, ranging from justifications for Hamas' involvement

in democratic elections, the violence of Zarqawi in Iraq and the legitimacy of the London bombings (Weimann, 2006; Conway, 2012). Weimann, for example, refers to the case of two extremist websites, *al-Tajdeed* and *al-Hesbah*, which accused each other of betrayal (Weimann, 2006). Therefore, if left unrestricted, a new cultural intelligence has the potential to strengthen and moderate the online community while marginalising extremist propagators (Ryan, 2007; Ali, 2008; Hussain & Saltman, 2014).

As is already becoming clear, advocates of soft approaches place a great deal of importance on the creation of counter-narratives. Briggs and Feve offer a useful definition, writing:

> Counter-narrative has become a catch-all term for a wide range of activities with different aims and tactics, everything from public diplomacy and strategic communications by government, to targeted campaigns to discredit the ideologies and actions of violent extremists (Briggs & Feve, 2013:i).

However, they also warn that "understanding about what works is still poor", and this largely remains the case today (Briggs & Feve, 2013:1). While counter-narrative campaigns may be full of positive messaging, it is almost impossible to gauge their effectiveness.

In his work analysing ISIS propaganda output, Winter offers a further criticism, bemoaning the lack of a deep enough understanding of "the motivations and objectives" that drive its media machine and the multiple and complex interplay of narratives that underpins it. Indeed, his study goes some way towards addressing this lack of knowledge, and Winter warns that any attempt to produce a single, all-encompassing counter-narrative simply will not work: "there is no 'Golden Fleece' solution to this problem. There is no one counter-narrative, nor is there any one audience that needs targeting" (Winter, 2015:8). In order for the international coalition against ISIS to see some success in its efforts to respond to the impact and efficacy of this propaganda machine, he calls for nothing less than a "complete restructuring" of the information architecture currently in place (Winter, 2015:8).

Some argue that, in order to counter the jihadist narrative, key tenets of the ideology should be attacked (such as theological justifications for violence) using altruistic beliefs, with sociological and psychological benefits provided instead (Briggs, 2011; Briggs & Feve, 2013; Hussain & Saltman, 2014; Aly et al., 2014). Aly et al. advocate for two kinds of disruption, or "noise." The first mimics approaches stated above, such as "planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning, and ultimately… behavior…" (Aly et al., 2014:35). The second is countering through "mechanical noise", or the "damaging of websites and the defacing and redirecting of users to the spreading of viruses and worms, blocking access, hacking, and total destruction" (Aly et al., 2014:35). While both have common-sense benefits and can be operationalised by state and non-governmental actors alike, it is also acknowledged that they remain tactical innovations that will provide a limited, short-term effect.

While counter-narratives are not a new approach, Archetti argues that the theory and conceptual approaches underlying them have not evolved adequately in line with the "reality of the digital age information environment where such tools need to be deployed" (Archetti, 2015:49). A lack of understanding persists regarding how propaganda and strategic communications influence individuals, and thus a rigorous analytical framework through which to empirically analyse success and failure remains elusive (Archetti, 2015: 49). Al Raffie stresses the importance of fully understanding not just the violent strand being countered, but also the foundational strands upon which it is formed. In the case of jihadism, "the Western world should do more in the way of understanding elements that Islamist and *jihadist* master narratives share" while being "wary of inadvertently advancing the causes of such groups" (Al Raffie, 2012:26).

Casebeer and Russell, however, warn of the scale of the task of understanding an ideology that is both transnational and stretches back through time, arguing that "confronting the Al Qaeda narrative must be a critical mission requirement of any strategy to confront the organization". Planners and policy-makers must therefore "come to terms with the phenomenon of Islamism or political Islam and

to understand how radicalized groups use violence to achieve ends related to the objectives of Islamism" (Casebeer & Russell, 2005:3). For them, a narrative's effectiveness depends on the strength of the storytelling that drives it: "given that stories are part and parcel of human cognition, we would also then expect consequently that stories might affect how these causes play out to germinate, grow and sustain terrorism" (Casebeer & Russell, 2005:3). This chimes with Nemr, who writes that "facts don't matter" when it comes to counter-narratives (Nemr, 2015).

This also relates to the critiques directed at 'Think Again Turn Away', which attempted to combat the ISIS narrative by providing facts about its barbarity. Referring to the initiative, Atran and Hamid ask, "Does it really matter to those drawn to the cause despite, or even because of, such things?" (Atran & Hamid, 2015). As Winter has stressed, brutality and war are explicit and active components of ISIS's messaging campaign (Winter, 2015:22, 26). For some, "strict obedience provides freedom from uncertainty about what a good person is to do" even if the obedience is to an abhorrent ideology (Atran & Hamid, 2015).

While Western governments have issued guidance on creating counter-narratives (Carpenter et al., 2009; RICU, 2010; NCTb, 2010b; HM Government, 2013), Archetti provides a convincing claim that they have yet to fully grasp the nature of the problem, or how to respond to it:

> To start with, from reports on how to counter 'online radicalization' to governments' calls for taking 'extremist material off the Internet', there is a strong focus on 'messaging.' Whether this means fighting the terrorists with the 'right' counter-message or removing 'their' extremist message, this approach reflects a woefully outdated model of public-media interactions (Archetti, 2015:50).

According to her, current approaches treat narratives as simple rhetorical devices and ignore the fact that they are also socially constructed. Thus, in order to achieve some level of resonance, they must

have deep roots within the social environment. Networks are therefore required for dissemination, a "constellation of relationships" that ensures that messages do not exist in a space devoid of meaning and context (Archetti, 2015:51). When developing counter-narratives, we must therefore be acutely aware of the "layered, asynchronous effects" which "will be difficult to coordinate and will involve multiple agents of action" (Casebeer & Russell, 2005:4). Such networks would aim to diminish the agents and "norm entrepreneurs" within their own borders, as identified by Al Raffie, who act as effective support structures for jihadist and Islamist narratives (Al Raffie, 2015:26).

There are signs, however, that our understanding of counter-narratives and how to effectively disseminate them may be gradually improving. While they cover much of what others have previously suggested and argued, Braddock and Horgan have contributed among the first theory-based, peer-reviewed frameworks for developing counter-narratives. The three by now familiar central components they identify are: "analyzing terrorist narratives… constructing counternarratives that challenge terrorist narratives… and disseminating the counternarratives to overcome barriers to persuasion" (Braddock & Horgan, 2016:381). Terrorist groups, according to them, "utilize an extensive range of communicative strategies to promote strategic objectives", while "narratives can be potent vehicles for persuasion" (Braddock & Horgan, 2016:381). However, they point out that, while some academics have provided practitioners with suggestions for developing relevant systems and stories for large counter-narrative campaigns, "guidelines related to the production of individual, small-scale counternarratives are nowhere to be found" (Braddock & Horgan, 2016:382).

Narratives are defined by Braddock and Horgan as "any cohesive and coherent account of events with an identifiable beginning, middle, and end about characters engaged in actions that result in questions or conflicts for which answers or resolutions are provided" (Braddock & Horgan, 2016:383). This definition crucially distinguishes a narrative's form from the ideas contained within it. Counter-narratives designed to contradict terrorist propaganda and discourage support for terrorism are constructed by identifying and

quantifying the most pernicious themes in the terrorist narratives, and targeting them by revealing the incongruities and contradictions in their coherence, or by disrupting "analogies that equate aspects of the narrative to real-world events" (Braddock & Horgan, 2016:388).

Assessing the best methods of counter-narrative dissemination largely relies on the nature of the milieu in which the narratives are being created. Among anonymous communicators who value independence, the producer of the counter-narrative must be considered genuine by the other participants. In milieus that value hierarchy and leadership, however, this producer must be both legitimate and identifiable (Braddock & Horgan, 2016:393). Indeed, the authors accept that these guidelines are just a first step, and that considerable research still needs to be done, though the paper represents a welcome effort to do so in a systematic, theory-driven manner.

INTELLIGENCE-LED APPROACHES

Advocates of the intelligence-led approach stress the importance of having a strengthened relationship between ISPs, social media companies and the police with adequate oversight in the hope that they can help facilitate cooperation against extremists (Bergin et al., 2009; Behr et al., 2013; Neumann, 2012; Neumann & Stevens, 2009). Others have taken a more transnational approach: fusion centres act as a 'check' on what users report on, and are a useful medium for facilitating the gathering of intelligence, monitoring and self-regulation of the Internet (Bergin et al., 2009).

The importance of remaining knowledgeable and aware of the extremist narrative that is being monitored on the Internet is often discussed. In the case of ISIS and the global jihad movement, it is mythic apocalyptic narratives of epic struggle and a utopianist renewal of society through the implementation of religious law (Winter, 2015; McCants, 2016). Retaining this knowledge reduces the possibility of 'fishing', or wasting time by not targeting and identifying areas where it is known that extremists operate and propagate their message (Bergin et al., 2009).

Intelligence can also be split into two different aspects: strategic and tactical. Strategic describes the process of acquiring intelligence on *how* extremists utilise the Internet, including what online platforms they are using, and potential changes of modus operandi (for example, lone-actor attacks) (Neumann, 2012). Equally important here is network analysis, which helps to reveal the connections between recruiters and sympathisers, as well as identifying key nodes that are involved in distributing information (Neumann, 2012). Another strategy identified for intelligence-gathering purposes is put forward by Moon, who, playing off the mimicry problem identified by Hegghammer, in which users of online forums struggle to build trust with each other due to the anonymity inherent in the medium, describes a process of online herding, or the use of doppelgangers to dupe extremist propagators (Moon, 2007; Hegghammer, 2014). Moon goes on to detail operational phases of how best to gather intelligence within the online community, with the ultimate goal of seeking to exploit it from within.

Tactical intelligence is described as the process of gaining intelligence on an imminent or planned attack. This may be more difficult to acquire, as terrorists will logically try to be more sensitive in revealing their plans online. However, Neumann states that even publicly available information from websites and online forums can turn out to be useful in foiling terrorist plots and preventing attacks. Lone actors are given as an example of violent extremists who leave plenty of virtual traces due to a general trend of being highly active on the Internet and receiving little by way of counter-intelligence training (Neumann, 2012:42). Following on from this would be the gathering of evidence to successfully prosecute an individual, or acquiring the legal justification to explore private online communications such as emails (Neumann, 2012).

Many scholars have explained the risks of such an approach, along with the possible legal obstacles, including the surveillance of transnational websites, the blurred lines between the public and private domain, and the unlawful and intrusive means that are an inherent element of monitoring (Neumann & Stevens, 2009; Hussain & Saltman, 2014). Other concerns revolve around

the lack of resources available to law enforcement agencies and the counterproductive dangers that feelings of stigmatisation may create among at-risk individuals within the community (Behr et al., 2013). Behr et al. state that monitoring and intelligence gathering is not the issue. Rather, they argue that law enforcement agencies are not able to actively bring the propagators to justice due to legal and resource barriers. Briggs explains how some international measures such as the Council of Europe's Convention on the Prevention of Terrorism have attempted to overcome these legal barriers by working within an international framework to conduct collective action and cooperation (Briggs, 2011).

The intelligence-led approach is popular and is driven by a belief that the Internet can, and should be, used as a means of gathering intelligence on extremist movements and propagators. In sum, "we can and should be using [terrorists'] online communications to learn as much as lawfully possible" (Romero, 2010:3).

CONCLUSION

THIS REVIEW HAS attempted to re-calibrate our conceptualisation of online radicalisation and the debates that accompany it. It has investigated the continued problem of definition, one that has haunted terrorism studies since its inception and continues to undermine both research and policy-making. It has surveyed the evolution of platforms that characterise the emergence of Web 2.0 and parsed out the increasingly atomised and novel ways in which information is produced and absorbed online. The material itself has retained its form, continuing to combine text, audio and video, although often in more polished and professionally produced ways.

The narratives share an increasingly symbiotic relationship with the platforms, however, applying constraints and creating opportunities for the individual in ways that the counter-extremism community is still attempting (and struggling) to understand. Meanwhile, the policy debate remains grounded in the nexus of the 'security versus civil liberty' debate, and the discussion on how to balance the two remains fraught.

Moving forward, it appears that the problem of definitions will remain an issue of contention for the foreseeable future. However, efforts can be made to mitigate this, starting with a renewed emphasis on method, on both a broad and narrow scale. An approach grounded in a vigorous empiricism can reveal nuances within an individual's radicalisation trajectory that often go unnoticed. This requires a skill set, namely open source data collection backed up by tailor-made analytical programmes and technologies. With an improved ability to harvest data from an individual's life, specifically from their online footprint, more accurate appraisals may be possible regarding behaviour. This systemised approach will allow for a consistency that bolsters analytical effectiveness over time as well as increasing the validity of conclusions.

Inroads have begun to be made here; Saltman and Smith's (2015) report on the radicalisation of female migrants to ISIS utilised these exact techniques and resulted in better understanding and explanations, not just of the radicalisation of the individuals, but their positions and level of influence within their networks. New data analysis platforms provide an opportunity to fill considerable gaps in

our understanding of how the content-platform nexus affects radicalisation, and a number of scholars have already taken advantage of this.

While this renewed empirical focus will give researchers the opportunity to more accurately analyse individual's trajectory toward violence, it will also provide a more nuanced understanding of the platforms themselves. Weimann's *New Terrorism and New Media* (2014) is a useful primer on how individuals interact with and use the novel functionality of each platform. It is notable for its singularity, but more nuanced analyses of the dynamic and evolving relationships between users and specific platforms is necessary, along with many groups and users' multi-platform strategies (Conway, 2017:83–85).

Research must also focus on developing a better understanding of why individuals who are operating in the same online environments and are exposed to the same materials do not engage in political violence.

When approaching the creation of narratives and counter-narratives, a more multi-disciplinary approach is necessary in order to understand how individuals interact and respond to these messages. However, Archetti offers as an encouraging lesson of the success of charities in creating viral campaigns that are able to thrive in an unpredictable online environment: "While they cannot know what is going to be 'liked' by the public and what will 'go viral' in an increasingly message-saturated society, they understand that most audiences generally do not 'buy' artificially-packaged top-down messages" (Archetti, 2015:55).

There remain, therefore, many avenues of important future research. Among the most pressing is a continued development of our understanding of how, if at all, online networks can replicate the influence on individual behaviour that physical, face-to-face interactions are already known to have. Related to this, there is significant scope to investigate if the Internet offers platforms that are conducive to the creation and adoption of new individual and collective identities. Research must also focus on developing a better understanding of why individuals who are operating in the same online environments and are exposed to the same materials *do*

not engage in political violence. A lack of such dependent variables in much of the data on this topic will continue to provide us with insufficiently comprehensive results from which to draw conclusions that can be useful for policy-makers.

At first glance, the information paradox – the more information one has on a subject does not necessarily provide clarity – appears to ring true with matters of online radicalisation. It has long been assumed that, given the sheer volume of information now consumed and produced by individuals on a daily basis, attempts to develop judgments on what does and does not influence them are futile. This has often resulted in research into online radicalisation losing its methodological grounding, leading to poor analysis and biased conclusions. With a renewed emphasis on empirical skills fit for the modern age, attempts can be made to understand an individual's radicalisation trajectory, thus opening the door for general trends to be better understood.

BIBLIOGRAPHY

Abdollahi, A., Cohen, F., Greenberg, J., Pyszczynski, T., Solomon, S., and Weise, D., 'Mortality Salience, Martyrdom, and Military Might: The Great Satan Versus the Axis of Evil', *Personality and Social Psychology Bulletin* 32(4), 2006, pp: 525–537

Abdullah-X, Homepage, 2016, www.abdullahx.com/

Ainsley, J.E., Volz, D., and Cooke, K., 'Trump to focus counter-extremism program solely on Islam – sources', *Reuters*, 2 February, 2017

Algemene Inlichtingen- en Veiligheidsdienst (AIVD), 'Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat', The Hague, 2006

Ali, S., 'Fighting Online Extremism: Tackling Old Challenges in the Internet Age', *RSIS Commentaries,* 2008

Al Raffie, D., 'Whose Hearts and Minds? Narratives and Counter-narratives of Salafi Jihadism', *Journal of Terrorism Research* 3(2), 2012, pp: 13–31

Alstyne, M., and Brynjolfsson, E., *Electronic Communities: Global Village or Cyberbalkans?,* MIT Sloan School, Cambridge, MA, 1997

Al-Suri, A., *The Call for Global Islamic Resistance* (2006)

Aly, A., 'The Terrorists' Audience: A Model of Internet Radicalisation', *Journal of Australian Professional Intelligence Officers* 17(1), pp: 3–19

Aly, A., Weimann, G., and Weimann-Saks, D., 'Making 'Noise' Online: An Analysis of the Say No to Terror Online Campaign', *Perspectives on Terrorism* 8(5), 2014, pp: 33–47

Amarasingam, A., 'An Interview with Rachid Kassem, Jihadist Orchestrating Attacks in France', *Jihadology,* 18 November, 2016

Amble, J.C., 'Combating Terrorism in the New Media Environment', *Studies in Conflict and Terrorism* 35(5), 2012, pp: 339–353

Anti-Defamation League (ADL), 'Poisoning the Web: Hatred Online', 2001

Anti-Defamation League (ADL), *Homegrown Islamic Extremism in 2013: The Perils of Online Recruitment and Self-Radicalization*, New York, 2014

Archetti, C., *Understanding Terrorism in the Age of Global Media: A Communication Approach* (New York: Palgrave MacMillan, 2013)

Archetti, C., 'Terrorism, Communication and New Media: Explaining Radicalisation in the Digital Age', *Perspectives on Terrorism* 9(5), 2015, pp: 49–59

Ashour, O., 'Online De-Radicalization? Countering Violent Extremist Narratives: Message, Messenger and Media Strategy', *Perspectives on Terrorism* 4(6), 2011, pp: 15–19

Atton, C., 'Far-right Media on the Internet: Culture, Discourse and Power', *New Media & Society* (8)4, 2006, pp: 573–587

Awan, A., 'Radicalization on the Internet? The Virtual Propagation of Jihadist Media and its Effects,' *Journal of the Royal United Services Institute* 152(3), 2007, pp: 76–81

Awan, A., Hoskins, A. and O'Loughlin, B., *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (London: Routledge, 2011)

Bakker, P., and Hille, S., 'Engaging the Social News User: Comments on News Sites and Facebook', *Journalism Practice* 8(5), 2014, pp: 563–572

Bartlett, J., and Littler, M., *Inside the EDL: Populist Politics in a Digital Age*, Demos, London, 2011

Bartlett, J., Miller, C., and Omand, D., *#Intelligence*, Demos, London, 2012

Behr, I., Edwards, C., Gribbon, L., and Reding, A., *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, RAND Europe, Brussels, 2013

Beirich, H., *White Homicide Worldwide: Stormfront*, Southern Poverty Law Center, 31 March, 2014, www.splcenter.org/sites/default/files/d6_legacy_files/downloads/publication/white-homicide-world-wide.pdf

Benson, D.C., 'Why the Internet is Not Increasing Terrorism', *Security Studies* 23(2), 2014, pp: 293–328

Bente, G., Frischlich, L., Rieger, D., *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*, Kolne, Wolters Kluwer: Luchterhand, Terrorism/Extremism Research Unit (*FTE*) of the German Federal Criminal Police Office *(Bundeskriminalamt)*, 2013

Bergen P., Hoffman B., Hurley M., and Suthers, E., *Jihadist terrorism: A Threat Assessment*, Bipartisan Policy Centre, Washington D.C., 2013

Berger, J.M., 'Tailored Online Interventions: The Islamic State's Recruitment Strategy', *CTC Sentinel* 8(10), October 2015, pp: 19–23

Berger, J.M., and Morgan, J., '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, March 2015

Berger, J.M., and Perez, H., *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, Washington D.C., February 2016

Bergin, A., Osman, S., Ungerer, C., and Yasin, A., *Countering Internet radicalisation in Southeast Asia*, Australian Strategic Policy Institute Special Report 22, 2009, pp: 1–24

Bermingham, A., Conway, M., McInerney, L., O'Hare, N., and Smeaton, A., 'Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation', *International Conference on Advances in Social Networks Analysis and Mining*, 20–22 July, 2009

Betz, D.J., 'The More You Know, the Less You Understand: The Problem with Information Warfare', *The Journal of Strategic Studies* 29(3), 2006, pp: 505–533

Bhatt, A., and Silber, M., *Radicalization in the West: The Homegrown Threat*, New York Police Department (NYPD) Intelligence Division, New York, 2007

Bjelopera, J., *American Jihadist Terrorism: Combating a Complex Threat*, CRS Report for Congress, 2013

Blee, K.M., *Women of the Klan: Racism and Gender in the 1920s*, Berkeley, CA: University of California Press, 1991

Bloom, M., 'In Defence of Honour: Women and Terrorist Recruitment on the Internet', *Journal of Postcolonial Cultures and Societies* 4(1), 2013, pp: 150–195

Borum, R., 'Understanding the Terrorist Mindset', *FBI Law Enforcement Bulletin*, 2003

Borum, R., and Gelles, M., 'Al-Qaeda's Operational Evolution: Behavioural and Organizational Perspectives', *Behavioural Sciences and the Law* 23(4), 2005, pp: 467–483

Boucek, C., 'The Sakinah Campaign and Internet Counter-Radicalisation in Saudi Arabia', *CTC Sentinel* 1(9), August 2008

Brachman, J., *Global Jihadism: Theory and Practice*, London: Routledge, 2009a

Brachman, J., 'The Pros and Cons with "Jihobbyism"', 2009b, http://jarretbrachman.net/the-pros-and-cons-with-jihobbyism/ [out of date URL; included here as this is where the term was coined]

Brachman, J., and Levine, A., 'You Too Can be Awlaki!', *The Fletcher Forum of World Affairs* 35 (1), 2011, pp: 25–46

Braddock, K., and Horgan, J., 'Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism', *Studies in Conflict & Terrorism* 39(5), 2016, pp: 381–404

Bradford, A., Frenett, R., and Hoyle, C., *Becoming Mulan? Female Western Migrants to IS*, Institute for Strategic Dialogue, London, 2015

Briggs, R., *Radicalisation: The Role of the Internet*, Institute for Strategic Dialogue: A working paper of the PPN, London, 2011

Briggs, R. and Feve, S., *Review of Programs to Counter Narratives of Violent Extremism*, Institute for Strategic Dialogue, London, 2013

Brown, I., *Internet Self-regulation and Fundamental Rights*, Index on Censorship, London, March 2010

Brown, I. and Cowls, J., 'Check the Web: The Ethics and Politics of Policing the Internet for Extremist Materials', *VOX-Pol*, 2015

Browne, R. and Cruickshank, P., 'US-led coalition targets top ISIS figure in Iraq strike', *CNN*, 15 February, 2017, www.cnn.com/2017/02/10/politics/coalition-strike-mosul-isis/

Bunt, G., *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments*, London: Pluto Press, 2003

Caiani, M., and Parenti, L., 'The Dark Side of the Web: Italian Right-Wing Extremist Groups and the Internet', *South European Society and Politics* 14(3), 2009, pp: 273–294

Calhoun, C., 'Indirect Relationships and Imagined Communities: Large Scale Social Integration and the Transformation of Everyday Life', in P. Bourdieu and J. S. Coleman (Eds.) *Social Theory for a Changing Society* (Oxford: Westview Press, 1991)

Callimachi, R., 'ISIS and the Lonely American', *The New York Times,* 28 June, 2015, www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html

Callimachi, R., 'Not "Lone Wolves" After All: How ISIS Guides World's Terror Plots From Afar', *The New York Times,* 4 February, 2017

Carpenter, J.S., Jacobson, M., and Levitt, M., *Rewriting the Narrative: An Integrated Strategy for Counterradicalization*, U.S. Presidential Task Force on Confronting the Ideology of Radical Extremism, The Washington Institute for Near East Policy, Washington D.C., 2009

Carter, J., Maher, S., and Neumann, P., *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, International Centre for the Study of Radicalisation, London, 2014

Carvalho, C., '"Okhti" Online: Spanish Muslim Women Engaging Online Jihad – a Facebook Case Study', *Online-Heidelberg Journal of Religions on the Internet* 6, 2014, pp: 24–41

Casciani, D., 'The Calgary Mother Fighting Radicalisation in Syria", *BBC News Magazine,* 5 May, 2015, www.bbc.co.uk/news/magazine-32539638

Casebeer, W.D. and Russell, J.A., 'Storytelling and Terrorism: Towards a Comprehensive 'Counter-narrative Strategy', *Strategic Insights* 6(3), Calhoun Institute, 2005, pp: 1–16

Chatham House, *Terrorism, Radicalization and the Internet,* Report of a private roundtable, Chatham House, London, 2008

Coates, J., *Armed and Dangerous: The Rise of the Survivalist Right*, New York: Hill and Wang, 1995

Cohen, F., 'Terrorism and Cyberspace', *Network Security* 5(31), 2002, pp: 17–19

Committee on Homeland Security House of Representatives (CHSHR), *Using the Web as a Weapon: The Internet as a Tool for Violent Radicalization and Homegrown Terrorism*, Hearing before the: Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 2007, pp: 1–6

Condon, C., and Weyers, J.R., 'The Newest Advertising and Recruiting Mogul: ISIS', *IBRABO,* June 2014, https://ibrabo.wordpress.com/2014/06/

Conway, M., and McInerney L., 'Jihadi Video and Auto-radicalisation: Evidence from an Exploratory YouTube Study', *First European Conference on Intelligence and Security Informatics* 3(5), 2008, pp: 1–11

Conway, M., 'From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Forum of Violent Radical Milieu', *Combating Terrorism Exchange* 2(4), 2012, pp: 12–22

Conway, M., 'From "Cyberterrorism" to "Online Radicalisation"', in Eid, M. (ed.), *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia*, Information Science Reference, 2014

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

Council on American Islamic Relations (CAIR), 'Brief on Countering Violent Extremism (CVE)', 13 October, 2016, www.cair.com/government-affairs/13063-brief-on-countering-violent-extremism-cve.html

Danish Security and Intelligence Service (PET), *Radikalisering og terror*, 2008

Department of Homeland Security (DHS), 'Terrorist Use of Social Networking: Facebook Case Study', 5 December, 2010, https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/

Della Porta, D., and LaFree, G., 'Processes of Radicalisation and De-Radicalisation', *International Journal of Conflict and Violence* 6(1), 2012, pp: 4–10

Della Porta, D., and Mosca, L., 'Searching the Net: Web Sites' Qualities in the Global Justice Movement', *Information, Communication and Society* 12(6), 2009, pp: 771–792

Douglas, K., Bliuc, A., Lala, G., McGarty, C., 'Understanding Cyberhate: Social Competition and Social Creativity in Online White Supremacist Groups', *Social Science Computer Review* 23(1), 2005, pp: 68–76

Ducol, B., 'Uncovering the French-speaking Jihadisphere: An Exploratory Analysis', *Media, War and Conflict* 5(1), 2012, pp: 51–70

Durodie, B., and Ng, S.C., 'Is Internet Radicalization Possible?', *RSIS Commentaries,* 2008

Edwards, C., and Gribbon, L., 'Pathways to Violent Extremism in the Digital Era', *The RUSI Journal* 158(5), 2013, pp: 40–47

Erelle, A., 'Skyping with the Enemy: I Went Undercover as a Jihadi Girlfriend', *The Guardian,* 26 May, 2015, www.theguardian.com/world/2015/may/26/french-journalist-poses-muslim-convert-isis-anna-erelle?CMP=fb_gu

EUROPOL, *Review 2013: General Report on EUROPOL Activities*, 2014, www.europol.europa.eu/content/europol-review-2013

EUROPOL, *EUROPOL's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda*, The Hague, 1 July, 2015, www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda

EUROPOL, *EU Internet Referral Unit: Year One Report*, The Hague, 22 July, 2016, www.europol.europa.eu/sites/default/files/publications/eu_iru_1_year_report_highlights.pdf

Fisher, A, and Prucha, N., 'Tweeting for the Caliphate: Twitter as the New Frontier for Jihadi Propaganda', *CTC Sentinel* 6(6), June 2013, pp: 19–23

Friedlander, S., *When you hear hoofbeats think of a zebra*, Costa Mesa, CA: Mazda, 1992

Furnell, S., 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium', *Computers and Security* 18(1), 1999, pp: 28–34

Gambhir, H.K., *Dabiq: The Strategic Messaging of the Islamic State*, Institute for the Study of War, 15 August, 2014, pp: 1–12

Geeraerts, S. B., 'Digital Radicalization of Youth', *Social Cosmos* 3(1) 2012, pp: 25–32

Gerdes, A., "Al-Qaeda on Web 2.0: Radicalisation and Recruitment Strategies", in Braman, J., Dudley, A., and Vincenti, G. (ed.), *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, Information Science Reference, 2012

Gill, P., Horgan, J., and Deckert, P., 'Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists, *Journal of Forensic Sciences* 59(2), 2014, pp: 425–435

Gill, P., Conway, M., Corner, E., and Thornton, A., 'What are the Roles of the Internet in Terrorism? Measuring Online Behaviours of Convicted UK Terrorists', *VOX-Pol Network of Excellence*, 2015

Githens-Mazer, J., and Lambert, R., 'Why Conventional Wisdom on Radicalisation Fails: The Persistence of a Failed Discourse', *International Affairs* 86(4), 2010, pp: 889–901

Gold, S., 'Virtual Jihad: How Real is the Threat?', *Network Security* 12 (1), 2012, pp: 15–18

Goldman, A., and Schmitt, E., 'One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program', *The New York Times,* 24 November, 2016

Goodwin, M., 'The Roots of Extremism: The English Defence League and the Counter-Jihad Challenge', *Chatham House Briefing Paper,* March 2013

Griffin, A., 'WhatsApp and iMessage Could Be Banned Under New Surveillance Plans*'', The Independent*, 12 January, 2015, www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html

Hale, W.C., 'Extremism on the World Wide Web: A Research Review', *Criminal Justice Studies* 25 (4), 2012, pp: 343–356

Halverson, J.R., and Way, A.K., 'The Curious Case of Colleen LaRose: Social Margins, New Media, and Online Radicalization', *Media, War & Conflict* 5(2), 2012, pp: 139–153

Hegghammer, T. 'Interpersonal Trust on Jihadi Internet Forums', in Gambetta, D. (ed.), *Fight, Flight, Mimic: Identity Signalling in Armed Conflicts*, (Oxford, Oxford University Press, 2014)

Hertfordshire Police, 'Counter Terrorism Internet Referral Unit (CTIRU)', www.herts.police.uk/advice/counter_terrorism.aspx

HM Government, *Tackling Extremism in the UK: Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism*, London, December 2013

Hjarvard, S., 'The Mediatization of Society: A Theory of the Media as Agents of Social and Cultural Change', *Nordicom Review* 29(2), 2008, pp: 105–134

Hoffman, B., 'The use of the Internet by Islamic extremists', Testimony presented to the United States House Permanent Select Committee on Intelligence, 4 May, 2006

Hoffman, B., Oral and Prepared Statement in 'Using the Web as a Weapon: The Internet As A Tool For Violent Radicalization And Homegrown Terrorism', Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, 6 November, 2006, https://fas.org/irp/congress/2007_hr/web.pdf

Hoffman, B., 'The Myth of Grass-roots Terrorism', *Foreign Affairs* 87(1), 2008

Hoffman, B., 'How Can I Miss You if You Won't Go Away?', *The National Interest*, 1 October, 2010, http://nationalinterest.org/blog/bruce-hoffman/how-can-i-miss-you-4166

Hoskins, A. and O'Loughlin, B., 'Media and the Myth of Radicalisation', *Media, War & Conflict* 2(2), 2009, pp: 107–110

Hughes, S. and Vidino, L., 'ISIS in America: From Retweets to Raqqa', George Washington University Program on Extremism, Washington D.C., December 2015

Hui, J., 'The Internet in Indonesia: Development and Impact of Radical Websites', *Studies in Conflict and Terrorism* 33(1), 2010, pp: 171–191

Hussain, G., and Saltman, E., *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it*, Quilliam, London, 2014

Institute for Strategic Dialogue (ISD), 'Case Study Report: Research Information and Communications Unit (RICU)', London, 2013, www.counterextremism.org/resources/details/id/413/research-information-and-communications-unit-ricu

Janbek, D.M., and Seib, P., *Global Terrorism and New Media: The Post-Al Qaeda Generation*, London: Routledge, 2010

Jenkins, B., *Stray Dogs and Virtual Armies: Radicalisation and Recruitment to Jihadist Terrorism in the United States since 9/11*, RAND Europe, Brussels, 2012

Jigsaw, 'Vision', Jigsaw homepage, https://jigsaw.google.com/vision/

Jones, D.M.J., and Smith, M.L.R., 'Paris Attacks: Is Radicalisation Really the Problem?', *The Telegraph,* 16 November, 2015, www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11997784/Paris-attacks-Is-radicalisation-really-the-problem.html

Katz, R., Oral and Prepared Statement on 'Using the Web as a Weapon: The Internet as a Tool for Violent Radicalization and Homegrown Terrorism', Hearing before the: Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, the Committee on Homeland Security, US House of Representatives, One Hundred Tenth Congress, 2007, pp: 14–34

Katz, R., 'The State Department's Twitter War With ISIS is Embarrassing', *Time,* 16 September, 2014, http://time.com/3387065/isis-twitter-war-state-department/

Kimmage, D., 'The Al-Qaeda Media Nexus', Radio Free Europe/Radio Liberty, Washington D.C., 2008a

Kimmage, D., 'Fight Terror With YouTube', *New York Times*, 26 June, 2008b, www.nytimes.com/2008/06/26/opinion/26kimmage.html?_r=0

Kirby, A., 'The London Bombers as 'Self-Starters': A Case Study in Indigenous Radicalisation and the Emergence of Autonomous Cliques', *Studies in Conflict and Terrorism* 30(5), 2007, pp: 415–428

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

Koehler, D., 'The Radical Online: Individual Radicalization Processes and the Role of the Internet', *Journal For Deradicalization* 1, Winter 2014/15, pp: 116–134

Kundnani, A., 'Radicalization: The Journey of a Concept', *Race and Class* 54(2), 2012, pp: 3–25

Lee, E., and Leets, L., 'Persuasive Storytelling by Hate Groups Online: Examining its Effects on Adolescents', *American Behavioural Scientist* 45(6), 2002, pp: 927–957

Levin, B., 'Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America', *American Behavioural Scientist* 45(6), 2002, pp: 958–988

Lia, B., *Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus'ab Al-Suri* (London: Hurst, 2009)

London, M., 'Why Tolerate Terrorist Publications?', *New York Times,* 23 January, 2015, www.nytimes.com/2015/01/24/opinion/why-tolerate-terrorist-publications.html?_r=0

Maher, S., Meleagrou-Hitchens, A., and Sheehan, J., *Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy*, International Centre for the Study of Radicalisation, London, 2012

Mahmood, S., *Online Social Networks: The Overt and Covert Communication Channels for Terrorists and Beyond*, Paper presented at IEEE Conference on Technologies for Homeland Security, 13–15 November, 2012

Malik, N., and Rafiq, H., *Caliphettes: Women and the Appeal of Islamic State*, Quilliam, London, November 2015

McCants, W., *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*, London: Picador, 2016

McCauley, C., and Moskalenko, S., 'Individual and Group Mechanisms of Radicalization', in *Protecting the Homeland From International and Domestic Security Threats,* Fenstermacher, L., Kuznar, L., Rieger, T., and Speckhard, A. (eds.), Air Force Research Laboratory, Washington D.C., 2011

McCauley, C., and Moskalenko, S., 'Mechanisms of Political Radicalization: Pathways Toward Terrorism', *Terrorism and Political Violence* 20(3), 2008, pp: 415–33

McDonald, M., 'Cyberhate: Extending Persuasive Techniques of Low Credibility Sources to the World Wide Web', in D. Schumann & E. Thorson (eds.), *Advertising and the World Wide Web* (Mahwah, NJ: Lawrence Erlbaum, 1999)

McFarlane, B., *Online Violent Radicalisation (OVeR): Challenges Facing Law Enforcement Agencies and Policy Stakeholders*, Monash University, 2010

Mealer, M.J., *Internet Radicalization: Actual Threat or Phantom Menace*?, Postgraduate Thesis, Naval Postgraduate School, Monterey, 2012

Meleagrou-Hitchens, A., *As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad*, International Centre for Study of Radicalisation, London, 2011

Michael, G., 'The New Media and the Rise of Exhortatory Terrorism,' *Strategic Studies Quarterly*, Spring 2013

Milton, D., *Communication Breakdown: Unraveling the Islamic State's Media Efforts*, CTC West Point, October 2016

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

Moon, D., *Cyber Herding: Exploiting Islamic Extremists' Use of the Internet,* US Naval Postgraduate School, Monterey, 2007

Moreng, B., 'ISIS' Virtual Puppeteers: How they Recruit and Train "Lone Wolves"', *Foreign Affairs*, 21 September, 2016

Nacos, B.L., 'Book Review: Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology by Awan, A., Hoskins, A., and O'Loughlin. B,' *Critical Studies on Terrorism* 4(3), 2011, pp: 473–476

Nacos, B.L. and Torres-Reyna, O., *Fuelling Our Fears: Stereotyping, Media Coverage, and Public Opinion of Muslim Americans*, Lanham: Rowman & Littlefield, 2007

National Coordinator for Counterterrorism (NCTb), *Jihadists and the Internet: 2009 Update*, The Hague, 2010a

National Coordinator for Counterterrorism (NCTb), *Countering Violent Extremist Narratives,* The Hague, 2010b

Nemr, C., 'Countering Islamic State Recruitment: You're Doing It Totally Wrong', *War on the Rocks,* 14 July, 2015, http://warontherocks.com/2015/07/countering-islamic-state-recruitment-youre-doing-it-totally-wrong/

Nesser, P., 'Joining Jihadi Terrorist Cells in Europe: Exploring Motivational Aspects of Recruitment and Radicalisation' in Ranstorp, M. (ed.), *Understanding Violent Radicalisation*, London and New York: Routledge, 2009

Nesser, P., Stenersen A., and Oftedal, E., 'Jihadi Terrorism in Europe: The IS-Effect', Perspectives on Terrorism 10(6), (2016)

Netherlands General Intelligence and Security Services (AIVD), *From Dawa to Jihad: The Various Threats from Radical Islam to the Democratic Order*, The Hague, December 2004

Neumann, P., *Countering Online Radicalization in America*, Bipartisan Policy Centre, Homeland Security Project, Washington D.C., 2012

Neumann, P., 'Options and Strategies for Countering Online Radicalization in the United States', *Studies in Conflict and Terrorism* 36 (6), 2013, pp: 431–459

Neumann, P., and Stevens, T., *Countering Online Radicalisation: A Strategy for Action*, International Centre for Study of Radicalisation, London, 2011

Neumann P., and Rogers, B., *Recruitment and Mobilisation for the Islamist Militant Movement in Europe,* King's College London, London, 2011

Newman, E., 'Exploring the 'Root Causes' of Terrorism', *Studies in Conflict and Terrorism* 29(8), 2006, pp: 749–772

OFCOM, 'Media Literacy Audit: Report on Adult Media Literacy', 2 March, 2006, www.ofcom.org.uk/research-and-data/media-literacy-research/adults2/medialit_audit

O'Hara, K. and Stevens, D., 'Echo Chambers and Online Radicalism: Assessing the Internet's Complicity in Violent Extremism', *Policy & Internet*, 7, 2015, pp: 401–422

O'Loughlin, B., Boudeau, C., and Hoskins, A., 'Distancing the Extraordinary: Audience Understandings of Discourses of "Radicalization"', *Continuum* 25(2), 2011, pp: 153–164

Pantucci, R., 'The Jihad will be YouTubed', *Foreign Policy,* 15 December, 2011, http://foreignpolicy.com/2011/12/15/the-jihad-will-be-youtubed

Park, J., and Suyin, Y., *Countering Internet Radicalisation: A Holistic Approach*, RSIS Commentaries, S. Rajaratnam School of International Studies, July 2010

Pearson, E., 'The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad', *Policy & Internet* 8(1), 2015, pp: 5–33

Precht, T., *Home Grown Terrorism and Islamist Radicalization in Europe: From Conversion to Terrorism*, Danish Ministry of Defence, December 2007

Prucha, N., 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram', *Perspectives on Terrorism* 10(6), 2016

Radicalisation Awareness Network (RAN), 'Proposed Policy Recommendations for the High Level Conference', December 2012a, www.counterextremism.org/download_file/59/134/308/

Radicalisation Awareness Network (RAN), 'RAN Internet and Social Media Working Group: Proposed Policy Recommendations', December 2012, www.counterextremism.org/resources/details/id/308/ran-internet-and-social-media-working-group-proposed-policy-recommendations

Ramsay, G., 'Conceptualising Online Terrorism', *Perspectives on Terrorism* 2(7), 2008, pp: 3–10

Ramsay, G., 'Relocating the Virtual War', *Defence Against Terrorism Review* 2(1), 2009, pp: 31–50

Ravndal, J.A., 'Anders Behring Breivik's Use of the Internet and Social Media' Journal Exit-Deutschland, Zeitschrift für Deradikalisierung und Demokratische Kultur, 2, 2013 pp: 172–185

Reitman, J., 'Jahar's World,' *Rolling Stone,* 17 July, 2013, www.rollingstone.com/culture/news/jahars-world-20130717?page=4

Research Information and Communications Unit (RICU), 'Prevent: A Communications Guide', 12 May, 2010

Rogan, H., *Jihadism Online: A Study of How Al-Qaida and Radical Islamist Groups Use the Internet for Terrorist Purposes,* Norwegian Defence Research Establishment, 2006

Rogan, H., and Stenersen, A., 'Jihadism Online', *FFI Focus* 1(8), 2008

Romero, D., 'Statement of Anthony D. Romero, Executive Director, American Civil Liberties Union before the House Committee on Homeland Security', American Civil Liberties Union, 26 May 2010

Royal Canadian Mounted Police (RCMP), *Radicalization: A Guide for the Perplexed*, June 2009

Russell, J., and Saltman, E., *The Role of Prevent in Countering Online Extremism* Quilliam, London, December 2014

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

Sageman, M., *Understanding Terror Networks*, Philadelphia, University of Pennsylvania Press, 2004

Sageman, M., *Leaderless Jihad: Terror Networks in the Twenty-First Century*, Philadelphia: University of Pennsylvania Press, 2008

Sageman, M., 'The Next Generation of Terror*', Foreign Policy*, 8 October, 2009, http://foreignpolicy.com/2009/10/08/the-next-generation-of-terror/

Saltman, E. and Smith, M., *Till Martyrdom Do Us Part: Gender and the ISIS Phenomenon*, International Centre for the Study of Radicalisation/Institute for Strategic Dialogue, London, 2015

Sanchez, S., 'The Internet and the Radicalisation of Muslim Women', Presentation at the annual meeting of the Western Political Science Association, Seattle, Washington, 2014

Schafer, J.A., 'Spinning the Web of Hate: Web-Based Hate Propagation by Extremist Organisations', *Journal of Criminal Justice and Popular Culture* 9(2), pp: 69–88

Schmid, A., *Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, ICCT Research Paper, March 2013

Selepak, A., '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), pp: 1–47

Silke, A., 'Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization', *European Journal of Criminology* 5(1), 2008, pp: 99–123

Singh, B., 'Youth Self-Radicalisation: Lessons from the Singapore Narrative', *Youth and Terrorism: A Selection of Articles* 87, 2009

Slater, M. D., 'Processing social information in messages: Social group familiarity, fiction vs. non-fiction, and subsequent beliefs', Communication Research, 17, 1990, pp: 327–343

Stevens, T., 'Regulating the 'Dark Web': How a Two-Fold Approach Can Tackle Peer-to-Peer Radicalisation', *The RUSI Journal*, 154(2), 2009, pp: 28–33

Suler, J., 'The Online Disinhibition Effect', *International Journal of Applied Psychoanalytic Studies* 2(2), 2005, pp: 184–188

The Redirect Method, Homepage, 2016, http://redirectmethod.org/

Thomas, T.L., 'Al Qaeda and the Internet: The Danger of "Cyberplanning"', *Parameters,* Spring 2003, pp: 113–123

Torok, R., 'Developing an Explanatory Model for the Process of Online Radicalisation and Terrorism', *Security Informatics* 2(6), 2013, pp: 1–10

Twitter, 'Combating Violent Extremism', 5 February, 2016, https://blog.twitter.com/2016/combating-violent-extremism

United Kingdom House of Commons Home Affairs Committee, *Memorandum: Post-Legislative Scrutiny of the Terrorism Act 2006*, London, September 2011

United Kingdom House of Commons Home Affairs Committee, *Roots of Violent Radicalisation*, Nineteenth Report of Session 2010–12, vol. 1, HC 1446, London, 6 February, 2012

United Kingdom House of Commons Home Affairs Committee, *Radicalisation: the Counter-Narrative and Identifying the Tipping Point*, Eighth Report of Session 2016–17, HC 135, London, 25 August, 2016

United States District Court for the Southern District of Ohio Western Division, Sentencing memorandum from USA vs. Munir Abdulkader, Case No. 1:16-CR-019, 10 November, 2016.

United States House of Representatives, Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security, 'Assessing and addressing the threat: defining the role of a national commission on the prevention of violent radicalization and homegrown terrorism', , One Hundred Tenth Congress, first session, 2007, pp: 6–14

United States State Department, 'A New Center for Global Engagement', January 2016, www.state.gov/r/pa/prs/ps/2016/01/251066.html [content removed]

United States Senate Committee on Homeland Security and Governmental Affairs (USSCHSGA), Majority and Minority Staff, *Zachary Chesser: A Case Study in Online Islamist Radicalisation and Its Meaning for the Threat of Homegrown Terrorism*, February 2012

Veldhuis, T., and Staun, J., *Islamist Radicalisation: A Root Cause Model*, Netherlands Institute of International Relations Clingendael, October 2009

Venhaus, J., *Why Youth Join Al-Qaeda*, United States Institute of Peace, May 2010

Vlahos, M., *Terror's Mask: Insurgency Within Islam*, John Hopkins University, May 2002, pp: 1–30

Walker, C., and Conway, M. *Online Terrorism and Online Laws*, Dynamics of Asymmetric Conflict 8(2), 2015, pp: 156–175.

Weimann, G., 'Virtual Disputes: The Use of the Internet for Terrorist Debates', *Studies in Conflict and Terrorism* 29(7), 2006, pp: 623–639

Weimann, G., 'Terror on Facebook, Twitter and YouTube', *Brown Journal of World Affairs* 16(2), 2010, pp: 45–54

Weimann, G., 'New Terrorism and New Media', The Wilson Center, *Research Series* 2, 2014, pp: 1–16

Weimann, G., 'Virtual Packs of Lone-wolves', The Wilson Centre, Washington D.C., 24 February, 2014, https://medium.com/its-a-medium-world/virtual-packs-of-lone-wolves-17b12f8c455a#.cl5wl5w51

Weimann, G., *Terrorism in Cyberspace: The Next Generation*, New York: Columbia University Press, 2015

White House, 'Empowering Local Partners to Prevent Violent Extremist in the United States', August 2011

Wiktorowicz, Q., *Radical Islam Rising*, Oxford: Rowman and Littlefield, 2005

Winter, C., *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*, Quilliam, London, July 2015

Wojcieszak, M., '"Don't Talk to Me": Effects of Ideologically Homogeneous Online Groups and Politically Dissimilar Offline Ties on Extremism', *New Media and Society* 12(4), 2010, pp: 637–655

Yasin, N.A.M., 'Online Indonesian Islamist Extremism: A gold mine of information', *RSIS Commentaries*, S. Rajaratnam School of International Studies, No. 144/2011, 2011

Zelin, A., *The State of Global Jihad Online*, New America Foundation, Washington D.C., 2013

The VOX-Pol Network of Excellence (NoE) is a European Union Framework Programme 7 (FP7)-funded academic research network focused on researching the prevalence, contours, functions, and impacts of Violent Online Political Extremism and responses to it.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312827

Email info@voxpol.eu
Twitter @VOX_Pol
www.voxpol.eu