

# Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies

Charlie Winter<sup>i</sup>

Charlie.winter@kcl.ac.uk

Peter Neumann<sup>i</sup>

Peter.neumann@kcl.ac.uk

Alexander Meleagrou-Hitchens<sup>ii</sup>

alexander.hitchens@kcl.ac.uk

Magnus Ranstorp<sup>iii</sup>

Magnus.Ranstorp@fhs.se

Lorenzo Vidino<sup>ii</sup>

vidino@gwu.edu

Johanna Fürst<sup>i</sup>

johanna.furst@kcl.ac.uk

<sup>i</sup> International Centre for the Study of Radicalisation (ICSR) at King's College London

<sup>ii</sup> Program on Extremism, George Washington University, Washington

<sup>iii</sup> Swedish Defense University, Stockholm

## Vol. 14(2)/2020

### The IJCV

provides a forum for scientific exchange and public dissemination of up-to-date scientific knowledge on conflict and violence. The IJCV is independent, peer reviewed, open access, and included in the Social Sciences Citation Index (SSCI) as well as other relevant databases (e.g., SCOPUS, EBSCO, ProQuest, DNB).

The topics on which we concentrate—conflict and violence—have always been central to various disciplines. Consequently, the journal encompasses contributions from a wide range of disciplines, including criminology, economics, education, ethnology, history, political science, psychology, social anthropology, sociology, the study of religions, and urban studies.

All articles are gathered in yearly volumes, identified by a DOI with article-wise pagination.

For more information please visit [www.ijcv.org](http://www.ijcv.org)

### Suggested Citation:

APA: Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: Research trends in internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence*, 14(2), 1-20. doi: 10.4119/ijcv-3809

Harvard: Winter, Charlie, Neumann, Peter, Meleagrou-Hitchens, Alexander, Ranstorp, Magnus, Vidino, Lorenzo, Fürst, Johanna. 2019. Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies. *International Journal of Conflict and Violence* 14(2): 1-20. doi: 10.4119/ijcv-3809



# Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies

Charlie Winter<sup>i</sup>

Peter Neumann<sup>i</sup>

Alexander Meleagrou-Hitchens<sup>ii</sup>

Magnus Ranstorp<sup>iii</sup>

Lorenzo Vidino<sup>ii</sup>

Johanna Fürst<sup>i</sup>

<sup>i</sup> International Centre for the Study of Radicalisation (ICSR) at King's College London

<sup>ii</sup> Program on Extremism, George Washington University

<sup>iii</sup> Swedish Defense University

## Abstract:

This article reviews the academic literature on how and for what purposes violent extremists use the Internet, at both an individual and organizational level. After defining key concepts like extremism, cyber-terrorism and online radicalization, it provides an overview of the virtual extremist landscape, tracking its evolution from static websites and password-protected forums to mainstream social media and encrypted messaging apps. The reasons why violent extremist organizations use online tools are identified and evaluated, touching on propaganda, recruitment, logistics, funding, and hacking. After this, the article turns to the ways violent extremist individuals use the Internet, discussing its role as a facilitator for socialization and learning. The review concludes by considering the emergent literature on how violent extremism is being countered online, touching on both defensive and offensive measures.

Keywords: radicalization, deradicalization, Internet, extremism, online extremism

The so-called digital revolution has changed the lives of people across the globe, and online and offline have become difficult to untangle. A great optimism that still existed in the 1990s has now evaporated: Everyone is aware that the Internet has not just created platforms for communication and cultural exchange, but it is also available to all those who consider cultural exchange and pluralism as wrong, and want to counter it. In many aspects extremists are some of the “early adopters” of the Internet, and it has long been inextricably linked with extremism, violent and otherwise (Meleagrou-Hitchens and Kaderbhai 2017; Ramsay 2013; Seib and Janbek 2010; Weimann 2006). With the dawn of the new millennium, the Internet has be-

come increasingly important for extremists around the world. Ever since it has been used for purposes such as planning terrorist attacks, as well as recruitment and financing and after the emergence of Web 2.0, this relationship was set to strengthen even further (Donelan 2009). Before long, all the mainstream social media and file-sharing platforms had been touched by extremist activism to some extent. Today, the Internet is no longer just one part of the spectrum of extremist activism – it has become a primary operational environment, in which political ideologies are realized, attacks planned, and social movements made.

While trends in online extremism are subject to constant and rapid evolution, there is no doubt that the Internet will remain of utmost importance to extremist causes across the ideological spectrum for decades to come – just as it will for everyone else that uses networked communication technologies. It cannot be inoculated from extremism: history shows that, as technology improves, extremists will adapt their approaches to optimally reflect the new operational environment and elude the measures working to undermine them. While the menace they present cannot be eradicated, it can be mitigated through informed policy choices.

Drawing on nearly two decades' worth of academic investigations into how extremists use online spaces, this review collects, surveys and digests the academic literature on extremism online, identifying both general dynamics and specific points of tactical and strategic evolution, guiding readers through the rich tapestry of research on the topic and providing a sense of the driving factors. Crucially, it illustrates that, much of the time, online extremism is simply intuitive usage of the Internet. Indeed, while it may be true that extremists use online spaces extensively, they are not always doing it in a way that is especially revolutionary.

The review begins with a brief definitional overview touching on terms like extremism and radicalization and proposing a definition of "online extremism" as *Internet activism that is related to, engaged in, or perpetrated by groups or individuals that hold views considered to be doctrinally extremist*. The next section takes a structural perspective, tracking tectonic shifts in how extremists have used online spaces since as far back as the 1980s. In the third and fourth sections, the review shifts its focus from structure to function: first, this is done from an organizational perspective – that is, the focus is on how and why extremist *organizations* use the Internet; and, second, it is done from the perspective of the user – that is, how and why *individuals* that are already extremist use the Internet. The last substantive section explores the literature regarding the other side of the equation: countering online extremism. The concluding section provides a set of policy-orientated recommendations drawn from the review.

It is worth noting that this text is largely – though not uniquely – confined to the topic of how jihadist organizations and individuals use the Internet. This is because, while almost all extremists make use of online spaces, the academic literature is skewed in favor of studies focusing on Islamist extremism (Meleagrou-Hitchens and Kaderbhai 2017). Rather than being down to the availability of data, this imbalance appears to be because, until 2019 at least, the security threat that other extremisms present has often been considered to be lesser than that posed by jihadist extremism. For this reason, there has tended to be less political appetite – and, accordingly, financial backing – for academic analysis of non-jihadist online extremism. Thus, although growing, especially in the wake of events like the 2019 Christchurch attacks, the literature remains relatively piecemeal.

## 1 Definitions

Before embarking on a discussion of extremism as it manifests in online spaces, it is first necessary to discuss just what exactly the term "extremism" means. In this section, we give an introductory overview of the most important academic discourses surrounding it, thereby providing readers with an understanding of its nuances and controversies. We conclude this part of the review by defining "online extremism" and "radicalization".

Scholars have disagreed about what constitutes extremism, violent extremism, terrorism, and radicalization for many years now, and for good reason – phenomena as complex as these demand comprehensive and continuous study. Without proper consideration of their nuances, discussion of such "morally loaded concepts" can give rise to "social judgment rather than the description of a set of phenomena" (Bonanate 1979, 197; Prus 2005, 49). None of these are static terms that describe today the same things that they did decades ago (Vermeulen and Bovenkerk 2012, 48). Rather, as social, political, economic, and security dynamics have transformed over the last two centuries, so too have their meanings as semantic categories evolved.

The word "extremist" is defined in the *Oxford Dictionary of English* as someone or something that "holds extreme political or religious views" (1st ed., 2010,

621). As Schmid points out, this means that the word “extremist” is, at base, a relative term, something that requires a benchmark “that is (more) ‘ordinary’, ‘centrist’, ‘mainstream,’ or ‘normal’ when compared with the (extreme) political fringe” (Schmid 2014, 11). In other words, as Neumann also notes, “extremism” can only be understood by comparing it with the accepted socio-political conventions of the day (Neumann 2013c). Hence, as our notions of what is “ordinary” have changed with time, what is regarded as “extremist” – let alone “terrorist” – has also fluctuated.<sup>1</sup> In that sense, all forms of “extremism” are context-specific.

In recognition of this, most scholars eschew a uniquely values-based definition of “extremism,” adopting instead a more flexible mode of categorization that can be used in the context of both actions (“behavioral radicalization”) and beliefs (“cognitive radicalization”) (Neumann 2013c, 873; 2013a, 4–5). For the likes of Neumann (2013a, 2013c), a group or individual can hold “extremist” views without necessarily undertaking “extremist” actions. For this reason, as Iannaccone and Berman also observe, “to equate religious extremism with religious militancy is a serious error” (Iannaccone and Berman 2006, 109–29).

Accounting for this, Wibtrope speaks of three categories of extremism: groups or individuals that have extreme objectives *and* use extreme means; those that have extreme objectives but do not use extreme means; and those that have conventional objectives but use extreme means to realize them (Wibtrope 2012, 79). If what is known today as violent extremism is encapsulated by Wibtrope’s first category, then non-violent extremism constitutes his second category.

For Neumann and Wibtrope, “extremism” refers to both an ideological persuasion *and* a range of activism. While useful, this distinction between doctrinal extremism and functional extremism is no panacea, especially when it comes to terrorism. This is because terrorism is both a tactic – that is, according to the definition adopted by the United States Department of State, “premeditated, politically motivated violence perpetrated against non-combatant

targets by sub-national groups or clandestine agents” (United States Department of State 2006) – and an ideological position – in Schmid’s words, “a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence” (Schmid 2013, 76). As many violent extremist groups refrain from using terrorism as a tactic due to its perceived ineffectiveness, it is imprudent to conflate the terms “terrorism” and “violent extremism” – they are patently not one and the same thing.

Having outlined what does or does not constitute extremism, we can now turn to the term “radicalization,” which has sparked even more controversy among scholars in recent years. In their brief review of the academic discourse around the term, della Porta and La Free note that it is variously understood to mean: “a process leading towards the increased use of political violence,” “an escalation process leading to violence,” and “the strategic use of physical force to influence several audiences” (della Porta and La Free 2012, 5, 7, 9). While it is obvious that these suggested definitions refer to different, although overlapping, phenomena, such semantic incoherence is found across the literature. All too often, the word is thrown around with little regard for the complexities to which it refers.

Recognizing its inadequacies as a catch-all expression, McCauley and Moskalenko conceive of it as a two-sided signifier: “Functionally,” they hold, it means “increased preparation for and commitment to intergroup conflict” (McCauley and Moskalenko 2008, 416). However, “descriptively, radicalization means change in beliefs, feelings, and behaviors in directions that increasingly justify intergroup violence and demand sacrifice in defense of the group” (McCauley and Moskalenko 2008, 416). Crucially, and in line with the above definitions of extremism, they do not contend that radicalization necessitates participation in illicit – read “extreme” – activities, let alone violence; indeed, they note that it can manifest itself in both nonviolent and violent political action (McCauley and Moskalenko 2010, 82).<sup>2</sup>

Neumann and Rogers, who define radicalization as the set of processes that causes attitudinal change

<sup>1</sup> In the United Kingdom in the 1920s, the suffragettes were routinely attacked as “terrorists” fighting for the “extremist” goal of votes for women.

<sup>2</sup> See also the article by Abay Gaspar et al. (2020) in this issue.

that leads towards the use of violence, take a similar tack (Neumann and Rogers 2011, 6). Through this lens, the term refers to a collection of mental and physical processes that can, but not always do, result in behavioral change. They caution that, while useful, this definition of radicalization still only partially solves the problem; even when understood like this, gathering all these processes under one umbrella term risks over-simplifying their complexities.

Rising to this lexical challenge, a significant number of theories of radicalization have been put forth. Perhaps the most prominent is that of Sageman, who posits that radicalization is predominantly a bottom-up process that occurs largely outside of the remit and influence of formal organizations (Sageman 2004, 2005, 2008). This reading of the phenomenon sees the social network as the most important catalyst, superseding external input from organizations and their officially designated recruiters. Often, this group “identity” is formed in opposition to an “other.” As Berger points out, in the particular context of Islamic State (IS) jihadism, the principal “out-groups” tend to be Shi’i Muslims and Jewish people; the latter are also one of the primary out-groups for American white supremacists, as Douglas et al. note (Berger 2017; Douglas et al. 2005, 68–76).

Wiktorowicz’s theory of extremist socialization, complements these ideas around identity formation, holding that, depending on individual circumstances, radicalization usually proceeds gradually and cumulatively – sometimes rapidly, but more often than not slowly (Wiktorowicz 2003, 2005). Moreover, Wiktorowicz holds, it can occur as a consequence of both passive and active interaction, a result of the continual adoption of norms, ideologies, and customs, all of which emerge from the individual’s staggered participation in the extremist milieu in question.

The likes of Hoffman, who sees radicalization as a top-down process that is hierarchically orchestrated on the part of the organization, approach the issue from a different angle (Hoffman 2017, 209–240; 2006, 2008). Similarly, Bergen, who has written extensively on terrorist recruitment, sees an instrumental role for the official outreach operative (Bergen et al. 2013). He notes that radicalization today is systematically augmented and amplified by “a virtual sea of jihadist re-

cruiters, cheerleaders, and fellow travelers who are available for interaction with him or her 24/7” (Bergen 2016).

While, for example, Amarasingam’s work on the IS’s Internet “family” dynamic and von Behr et al.’s exploration of radicalization online supports the bottom-up readings of radicalization espoused by Sageman and Wiktorowicz, so too does Berger’s investigation into IS’s online micro-community do much to evidence Hoffman’s conceptualization (Amarasingam 2015; von Behr et al. 2013; Berger 2015).

At this juncture, we can (re)define the term “online extremism” as Internet activism that is related to, engaged in, or perpetrated by groups or individuals that hold views considered to be doctrinally extremist. This definition thus includes the first two of Wibtrope’s categories – the activities of non-violent extremists and violent extremists, but not terrorists. It is consciously context-specific, and relevant only in relation to social conventions at the time and place in which the group or individual in question exists. While imperfect, this concession to historical context is a necessary evil. For its part, “radicalization” – which should never be confused with recruitment because it refers to things that often precede an individual actually joining an extremist organization – is defined as the set of processes by which one comes to engage in doctrinal extremism of any form, whether online or otherwise. As Neumann (2013c, 878) points out, just like the term “extremism,” it is “inherently context-dependent, and its meaning will always be contested.” Whichever definition one opts for, though, the process rarely, if ever, happens uniquely online, so, below, the term “online radicalization” is avoided.

As the rest of this review demonstrates, however we choose to define extremism or radicalization, the Internet has become a central theatre of operations for the former, and a key facilitator for the latter. While, as O’Hara and Stevens and Archetti have highlighted, no causal relationship necessarily exists between it and either phenomenon, there is no question that extremist organizations would not be where they are today without their adept use of virtual terrains (Archetti 2018, 8; O’Hara and Stevens 2015; Stevens and O’Hara 2015). This should not come as a surprise. Indeed, as Benson notes, “it would be strange if to-

day's terrorist did not use the Internet, just as it would be strange if past terrorists did not use the postal service or the telephone" (Benson 2014).

## 2 The Virtual Landscape

Online extremism has developed in leaps and bounds in recent decades, reflecting advances in technology and shifts in both the physical and information security environment. This section offers a review of the literature regarding the structural side of online extremism: it maps developments in the extremist ecosystem since the emergence of the Internet as we know it today, drawing on nearly two decades' worth of academic inquiry.

As far back as 1985 – that is, five years before the term “World Wide Web” had even been coined – right-wing supremacists in the United States had established the “White Aryan Resistance” platform, an online bulletin board devoted to sharing news, facilitating recruitment, and disseminating instructional materials (Smith 2017). In the years that followed, others followed suit, enjoying the relative freedom with which they could communicate and cultivate their causes online.

As research by Gerstenfeld et al. finds, during the first decade and a half of the Internet, extremists tended to have four key objectives online: increase their international appeal; recruit new individuals; network with likeminded groups; and engage in image management (Gerstenfeld et al. 2003, 37–40). In 2004, Weimann comes to a similar, albeit more expansive, conclusion (Weimann 2004). He contends that the Internet has become instrumental to extremists – in this case, those that also engage in terrorism – because it allows them to: conduct psychological warfare; produce and publish propaganda; mine sensitive data; raise funds and accumulate resources; recruit and mobilize new supporters; network with other organizations; share logistical information; and plan and coordinate attacks (Weimann 2004, 5–10). Focusing their attention on white supremacist extremists in the early to mid-2000s, Simi and Futrell advance Weimann's findings, noting that static websites in particular were “very influential in movement members' efforts to construct and sustain movement culture and collective action” (Simi and Futrell 2006, 116).

Conway, building on this research, also contends that online activism was “an unmitigated success” for extremists, especially in terms of propaganda dissemination and information provision through static websites (Conway 2005).

Despite unforeseeable technological advances, extremists of today – whether they are white supremacists, radical leftists, or Salafi-jihadists – use the Internet to achieve the very same objectives outlined by Gerstenfeld et al. in 2003, Weimann in 2004, and Conway in 2005. While organizationally administered static websites – which, to be sure, are still in scaled-down operation today – were in vogue for a time, they turned out to be imperfect vehicles for ideological incubation. As Atton notes in the context of British right-wing extremism, as hierarchically organized platforms they by definition left those in charge with “a hegemony of ideas,” which stymies individual participation (Atton 2006). As Zelin found, after more than a decade prioritizing static websites over other digital communication tools, jihadist extremists had also begun to shift onto online forums by the mid-2000s (Zelin 2013). Besides being a more secure way to disseminate propaganda and share instructional advice, these new platforms were advantageous for another reason: a virtual sense of jihadist community – identity, even – had begun to blossom on them.

Weimann points out that jihadist extremists would use virtual safe-havens such as these to gather together online, engaging in spiritual argumentation, exchanging news, and swapping notes on things like poetry (Weimann 2006). Moreover, as Kimmage (2010) and Torres-Soriano (2016) separately document, they would also engage in ideological disputes with other members and even leaders of the very movements to which they “belonged” (Kimmage 2010). Thus, just as the advent of the interactive Internet revolutionized how non-extremists interacted, so too did it transform the jihadist information landscape.

To be sure, jihadist forums – which, as Zelin is careful to point out, were always used most enthusiastically by Arabic-speakers (Zelin 2013) – were not just important at the level of the user; they also served as organizational mouthpieces (Renfer and Haas 2008). Official spokespeople used them to deride internal rivals and lambast adversaries, keeping hold of “the at-

tion of the faithful” and making sure that their adherents stayed in line with the ideological parameters of the day (Kamolnick 2017; Kimmage 2010, 2; Wage-makers 2011). Lia and Hegghammer document how forums were also used for hosting virtual town hall meetings, wherein strategic and tactical advice could be crowd-sourced and integrated into attack-planning (Lia and Hegghammer 2010). Above all, though, the forums were most important to jihadist groups as places where propaganda could reliably and safely be disseminated (Kimmage 2008).

Notwithstanding their comparative advantage over static websites, forums were not without their disadvantages either, and, as both Torres-Soriano and Zelin have shown, the forum frenzy was largely over by 2013 (Torres-Soriano 2012). Groups like al-Qaida (AQ) and al-Shabab had spotted an opportunity elsewhere, and were spending less time trying to attract new adherents to this password-protected network.<sup>3</sup> Instead, they had begun to shift their attention to more mainstream – read “accessible” – platforms, social media networks like Twitter, Facebook, and VKontakte, and file-sharing hubs like YouTube (Weimann 2010; al-Shishani 2010; Prucha and Fisher 2013; Johnson et al. 2016; Manrique et al. 2016).

This ideology-wide migration began to occur in earnest after al-Shabab became the first terrorist group in history to live-tweet one of its operations. Berger and Stern describe how the group used Twitter to provide tactical updates on the attack it mounted against the Westgate Shopping Mall in Nairobi, Kenya, in September 2013, as does Sullivan (Berger and Stern 2015, 163; Sullivan 2014).

In the aftermath of events like Westgate, jihadist use of Twitter swelled almost exponentially. By 2014, all the major organizations were heavily invested in the platform. As a result of this and the easier access to data that it afforded, the amount of academic scrutiny to which their online activities were subjected flourished – scholars now had more access to empirical data than ever before. Carter, Maher, and Neumann’s 2014 report is a paradigmatic example of this new research trajectory (Carter, Maher, and Neumann 2014). Using social network analysis software Palantir

<sup>3</sup> It should be noted that, while this may well have been the case for the extremist majority, an old guard of jihadists kept them alive long into the 2010s.

to determine key focal points in online extremist networks associated with Syrian jihadist groups like Jabhat al-Nusra and the Islamic State of Iraq and ash-Sham (as they were known at the time), the study provides granular insight into an ecosystem that had hitherto been out of the reach even of governments. Following in their footsteps were the likes of Klausen, who also used quantitative social network analysis techniques to dissect the global jihadist advocacy network, and Berger and Morgan, whose ground-breaking census of pro-IS Twitter users found that there were no fewer than 46,000 such accounts operating between September and December 2014 (Klausen 2015; Berger and Morgan 2015). Studies like these revealed that there had been a tectonic shift in the online jihadist landscape. No more did it constitute a closed network of forums predominantly populated by Arabic-speakers; – instead, it had become a global hive of political activism and cultural exchange (Zelin 2013, 7). It is worth noting as an aside that scholars have long turned to this form of social network analysis as a way to analyze online extremism. As far back as 2000, for example, Burris, Smith, and Strahm used it to examine the “organizational and mobilizational structure” of the virtual white supremacist movement (Burris, Smith, and Strahm 2000, 215), which they found to be decentralized and subject to constant change.

This evolution did not stop there. By the end of 2015, another transformation had been wrought in the fabric of online jihadist activism. As government pressure mounted in response to the increasingly audacious attacks launched by IS members and supporters, social media corporations and file-sharing hubs began to crack down on jihadists using their platforms. Their decline on mainstream services such as Twitter was precipitous, a result of the sustained “suspension pressure” caused by algorithm-assisted account censorship (Milton 2016; Berger and Perez 2016; Berger 2016).<sup>4</sup> However, while it may have been shrinking, the jihadist ecosystem was not disappearing – it was simply changing. Indeed, in response to these measures (which are further discussed below),

<sup>4</sup> It is worth noting that the decline of the Islamic State on Twitter coincided with a massive increase in the use of the platform by white nationalists, as is also demonstrated in research by Berger (2016).

the community had once again migrated elsewhere, this time to services like Telegram, a hybrid social networking platform that proved to be ideal for peer-to-peer communication, group discussions, and propaganda dissemination (see Johnson et al. 2016; Manrique et al. 2016). At the time of writing, academic explorations of Telegram – which is now widely regarded as jihadists’ preferred platform – are few and far between (exceptions: Bloom, Tiflati, and Horgan 2017 for a descriptive account; Stalinsky and Sosnow 2017 for an operational overview).

By the beginning of 2018, there were signs that another migration was on the horizon. For more than two years, pressure had been mounting on Telegram to cleanse itself of jihadists, and, contemporaneously, a raft of other encrypted and privacy-maximizing platforms – like, for example, Zello, Threema, Wickr, and Surespot – had begun to emerge as online gathering points (Katz 2016). While Telegram’s attempts to inoculate itself have so far yielded little meaningful progress, history shows that, if the pressure mounts enough, its jihadist users could one day end up abandoning the platform entirely. Where they will go is, as yet, a mystery. However, the recent work of Weimann, which looks at terrorism on the Dark Web, coupled with Brantly’s account of how extremists use encryption, could provide some clues (Weimann 2016; Brantly 2017).

### 3 How and Why Extremist *Organizations* Use the Internet

Having established a broad sense of how extremists shifted their activities away from static websites and forums to social media platforms and file-sharing hubs, the issue of online extremism can now be examined from a more functional perspective (Kimmagine 2008; Rogan 2006; Rudner 2016). In this section, the academic literature on how extremists use online spaces at an organizational level is reviewed. The literature is broken down into four distinct but overlapping themes: propaganda, recruitment, logistics and planning, and funding.

#### 3.1 Propaganda

Many scholars have furthered our understanding of the strategic logic behind the online dissemination of

propaganda, especially by jihadists. Wagemakers’ study into Abu Jandal al-Azdi, one of AQAP’s most important Internet ideologues, offers crucial insight into the editorial thinking behind jihadist public diplomacy (Wagemakers 2011). Similarly useful are Anzalone’s works into al-Shabab’s strategic communication operations, both of which demonstrate that IS is far from the only jihadist group to have a sophisticated grasp of editing software, sound syncing, and narrative structures (Anzalone 2010, 2016). Sidestepping AQ and its affiliates, Mozes and Weimann investigate how the Palestinian Islamist group Hamas has used the Internet to brand and facilitate its activism, in a study which represents one of the most effective conceptual investigations of extremism online to date (Mozes and Weimann 2010). Their approach is echoed by Neil Aggarwal’s psychiatry-informed exploration of the Afghan Taliban’s “virtual emirate” and Khatib’s account of Hizbullah’s image management operations in Lebanon and beyond, both of which draw relatively similar conclusions – that there are striking similarities between the virtual branding of extremist insurgencies and international businesses (Aggarwal 2016; Khatib 2013). For his part, Holbrook focuses his attention on both far-right *and* Islamist propaganda activism, subjecting a spectrum of extremist “discourses” to comparative analysis in order to identify and assess “similarities and differences and the ways in which the former has reacted to the latter” (Holbrook 2013, 218). Like Berger (2017), he notes that a consistent in-group/out-group dynamic exists across the extremist spectrum, serving as an ideological glue for adherents of the movement.

Predictably, IS propaganda has drawn by far the most attention in recent years, something borne of the fact that its media output has been more accessible and more immediately important to policymakers. Investigations into its communication strategy can be split into two: explorations of strategic doctrine, and content analyses. Farwell’s 2014 contribution, which contends that “the group’s main tool has been brute force,” puts forth a relatively crude and emotional account of its understanding of strategic communication (Farwell 2014, 49–55). More informative is Ingram’s discussion of the logic underpinning its approach, which, when read alongside Philips, who con-



tends that IS deploys a distinctly revolutionary approach to propaganda in warfare, provides a wide-ranging and nuanced account of how and why the self-proclaimed caliphate communicates in the way it does (Ingram 2015; Phillips 2017). Noting in particular its synthesis of global and local narratives in order to cater to a “glocal” constituency, Ingram demonstrates a sophisticated awareness of how media operations can be used in warfare (Ingram 2015, 731). Works by Gambhir and by Gartenstein-Ross, Barr, and Moreng, approach the issue from a similar angle, though their accounts operate more at the tactical level (Gambhir 2016; Gartenstein-Ross, Barr, and Moreng 2016).

Broadly speaking, there are two types of content analysis of IS media: those addressing aggregate output, and those focusing on just one or two types of its propaganda in particular. Zelin’s 2015 work, which examines IS’s official output over the course of a single week in May of that year, was the first archival exploration of its kind (Zelin 2015). It is complemented by Winter’s studies from 2015 and 2016, which find, like Zelin’s, that IS’s appeal rests on much more than the violence for which it is most famous (Winter 2015a, 2015b, 2016). Instead, these accounts suggest, it was in large part its promise of utopia that attracted recruits. Moreover, as research by Sheikh indicates, not only did it help recruit new adherents, it also kept the organization’s ranks coherent (Sheikh 2016).

The second type of content analysis considers specific aspects of IS’s media output in isolation. With their typology of execution videos, Chouliaraki and Kissas offer a fascinating account of IS’s understanding of spectacle and “horrorism,” while both Winkler and Adelman work to disentangle the strategic meaning of its infographics (Chouliaraki and Kissas 2017; Winkler 2016; Adelman, 2018). For his part, al-Rawi analyses the logic of provocation behind the trailer for a never-released IS computer game, *Salil as-Sawarim* (Al-Rawi 2016). While his conclusions are somewhat problematic – given that the game was never actually released, its trailer is of dubious importance – they are useful if nothing else because they are reminiscent of Selepak’s earlier work on the video games found on white supremacist websites, in which he warns of their ability to desensitize players to the use of violence (Selepak 2010). Winkler et al.’s analysis of

Zelizer’s “about to die” trope (2010) in images within the magazine, which goes beyond the descriptive to examine how and why *Dabiq* magazine is structured in the way it is, is one of the most revealing assessments (Winkler et al. 2016). O’Halloran et al., who use *Dabiq* as an opportunity to develop a multi-modal approach for the study of mixed-media propaganda, also examine how meaning is constructed in its pages (O’Halloran et al. 2016). Ingram, whose comparison of *Dabiq* and *Inspire* adds a further layer of contextual analysis, takes a different approach, using these magazines as a lens through which to explore ideological rivalry between their two publishers, al-Qa’ida in the Arabian Peninsula (AQAP) and IS (Ingram 2016b).

### 3.2 Recruitment

The next prong of the organizational literature concerns charismatic engagement. Conway and Gendron, both of whom examine the role of charisma, and whether or not it transmits online, focus their attention on the online recruitment activities of AQAP. Conway argues that this alone will not result in the formation of radical milieus, let alone recruitment (Conway 2012, 12–22). Rather, she holds, a measure of face-to-face interaction is required to facilitate the process of joining an extremist organization. Interestingly, she also notes that “the [I]nternet plays a greater role in violent jihadi radicalization processes in Western countries than in other parts of the world” (Conway 2012, 8), an assertion that seems to be as relevant today as it was six years ago. Gendron examines the role of AQAP “recruiting sergeant” Anwar al-Awlaki, finding that his charismatic appeal was strengthened by the Internet (Gendron 2017). This thesis is reiterated in both Shane’s and Meleagrou-Hitchens’s accounts of al-Awlaki’s history and ideological evolution, not to mention Ingram and Whiteside’s brief exploration of his enduring post-assassination influence (Shane 2016; Meleagrou-Hitchens 2012; Ingram and Whiteside 2017).

In the specific context of IS, the issue of organizational recruitment has mainly remained the remit of journalists, foremost among them Callimachi and, to a lesser extent, Feuer and Taub (Callimachi 2015, 2017; Feuer 2018; Taub 2015). That being said, Berger’s aforementioned investigation of IS’s online micro-

community, Gates and Podder's assessment of its bifurcated recruitment strategies (that is, one for local fighters, and another for foreigners), Reynolds and Hafez's analysis of how social media networks do or do not play a role in the recruitment of German fighters, and Winter's account of how it synthesizes community, propaganda, and instructional advice in order to attract new blood from as far afield as Australia represent four notable exceptions to this rule (Berger 2015; Gates and Podder 2015; Reynolds and Hafez 2017; Winter 2016).

### 3.3 Logistics and Planning

A small number of detailed exploratory investigations have been conducted into how – at an organizational level – online spaces are used to facilitate terrorism. Hughes and Meleagrou-Hitchens, for example, map IS's "virtual entrepreneur" network, an issue that is also addressed in a series of articles by Gartenstein-Ross, Barr, and Blackman (Gartenstein-Ross and Blackman 2017; Gartenstein-Ross and Barr 2016; Hughes and Meleagrou-Hitchens 2017). Each of these investigations asserts the existence of a convoluted logistical system that sees in-theatre IS fighters encouraging, motivating, inciting, and instructing would-be attackers outside of Syria and Iraq.

Focusing on how organizations communicate operational advice through the Internet, there are the likes of Kenney, and Reed and Ingram. The former's account of the limitations of bomb-making literature for educating would-be attackers makes for an invaluable addition to the literature on terrorist innovation (Kenney 2010). For their part, Reed and Ingram compare and evaluate the tactical effectiveness of and strategic objectives behind *Inspire* magazine's "Open Source Jihad" and *Rumiyah*'s "Just Terror" sections (Reed and Ingram 2017). In each case, they contend, instructional materials are important not just for the logistical advice they offer, but also for the strategic value with which they are imbued, which is used as a means with which "to legitimize, justify and inspire engagement in violence [as well as] inspire a "copycat" effect in audiences while reinforcing the group's overarching message" (Reed and Ingram 2017, 12–13).

### 3.4 Funding

The final prong of the literature on organizational online extremism line focuses on how the Internet factors into fundraising operations. Noting that more "accessible" issues like propaganda and recruitment tend to receive the bulk of the analytical attention, Jacobson contends that terrorist groups across the ideological spectrum also use online spaces to facilitate illicit transactions and fund overseas activities (Jacobson 2009). Focusing their attention on how jihadist fundraisers make use of social media to solicit funding from volunteer supporters, researchers at the Camstoll Group assert that "al-Qaida and ISIS fundraisers have taken credit for millions of dollars raised using social media-based campaigns" (Camstoll Group 2016, 2). While their case studies make for interesting reading, they do not serve as robust evidence for the claims of "millions of dollars," and should thus be treated with caution. Investigations by Salami and by Goldman et al. tackle an even more elusive aspect of terrorist financing, offering speculative analysis as to how crypto-currencies could one day be used to facilitate terrorist activism (Salami 2017; Goldman et al. 2017). While both accounts struggle to move beyond the anecdotal, they highlight important vulnerabilities in the financial system and could one day prove to have been prescient.

## 4 How and Why Extremist Individuals Use the Internet

Sidestepping the top-down perspective, many scholars have opted to explore online extremist activism at the level of the user. Even the most cursory glance at this cross-section demonstrates that, much of the time, extremist individuals use the Internet for the very same reasons that "normal" people use it – anything from basic social interaction to political activism and exchange. While the body of literature examining this side of the online extremism spectrum is increasingly large, it remains waylaid by a generalized shortage of data regarding the processes by which the "supply side," as discussed above, impacts on the "demand side," as discussed below (von Behr et al. 2013).

#### 4.1 Radicalization

Most scholars agree that the Internet does not cause radicalization. In the course of their dismissal of this idea, Hoskins and O’Loughlin express deep unease regarding what they call “the online/offline distinction” (Hoskins and O’Loughlin 2009, 109). Essentially, their position is that the term “online radicalization” is a misnomer and, ultimately, not representative of reality. Likewise, Gill, Corner, and Conway refer to the “false dichotomy” of the distinction, which neatly – and unrealistically – separates online processes of radicalization with those that take place offline (Gill et al. 2017, 114). With this in mind, most investigations into online extremism at the level of the user work with the assumption that radicalization, while it can be impacted by things that happen online, does not come purely as a result of online behaviors. Indeed, it is usually taken as a given that online processes, interactions and activities complement but do not substitute their offline counterparts, and that there is little sense in attempting to distinguish one sphere from the other.

Focusing in particular on how propaganda contributes to the individual’s journey into extremism, Weisburd’s analysis of visual motifs in jihadist and street-gang videos is an innovative exploration, although it spends more time developing a categorization for violent footage than examining its actual impact on the consumer (Weisburd 2009). Reiger, Frischlich, and Bente’s assessment of the psychological impact of consuming propaganda is more insightful (Reiger, Frischlich, and Bente 2013). Building off a study of some 450 individuals, they demonstrate that there is no simplistic or predictable reaction to propaganda, and that its consumption *alone* does not usually cause radicalization. With their dataset of 6,020 respondents, Pauwels and Schils come to a similar conclusion (Pauwels and Schils 2016). Communication scholar Archetti holds a comparable position but goes even further, pointing out that there is a “tendency to assume that the mere existence of propaganda material equals consumption by audiences and influence on them,” a warning that counter-terrorism policy-makers and counter-strategic communications practitioners alike would do well to heed (Archetti 2013).

Sidestepping the study of propaganda, other scholars have attempted to shed light on how the Internet impacts radicalization processes by examining relational dynamics between online extremists. Hegghammer’s investigation into when, how, and why jihadists manage to forge trusting relationships with each other over the Internet highlights the lengths individual users go to to verify, vet, and validate themselves and their associates (Hegghammer, n.d.). Geeraerts is similarly interested in inter-personal dynamics in online extremist “echo rooms,” contending that online friction over personal credibility can lead to a strengthening of extremist attitudes (Geeraerts 2012, 26). For his part, Shortland also examines extremist community dynamics, albeit from a different angle – that of counter-terrorism policy (Shortland 2016). He contends that gauging intent from vague pronouncements made on social media is a difficult, if not impossible, task, given the persistent “lack of understanding related to the interaction of online and offline experiences” (Shortland 2016, 591).

Focusing their attention on the role of online education and instruction in radicalization, some scholars have examined the antecedent behaviors of terrorists and would-be terrorists. Freiburger and Crane are among the first to approach it from a social learning perspective (Freiburger and Crane 2008). Taking a different approach that is specifically focused on pre-attack preparation and learning, Stenerson, Kenney, and Holbrook have all examined the literature on bomb-making made available by terrorist organizations, attempting to gauge how useful it actually is for would-be attackers (Stenerson 2013; Kenney 2010; Holbrook 2015). They broadly agree that, while they make for sensational headlines, actually learning from such manuals is easier said than done because the bomb-making “process is not all that simple or straightforward” (Holbrook 2015, 131). Elsewhere, Holbrook investigates jihadist literary tastes by analyzing texts seized during counter-terrorism investigations in the United Kingdom (Holbrook 2017). Reviewing no fewer than 1,700 media publications, Holbrook notes that the ideological current extends beyond known celebrities of jihadist extremism like al-Awlaki, and that works of theology from many hundreds of years ago

can still be found on the virtual bookshelves of violent extremists today.

Widening the remit to examine online behaviors from a more general perspective are Gill et al., who find no causal link between the rise of the Internet and lone-actor terrorism between 1990 and 2011 (Gill et al. 2017). However, online spaces do still serve as an important – though not always necessary – logistical pillar for terrorism planning (Gill, Horgan, and Deckert 2014). As Ravndal points out, though, not all terrorists exhibit clear pre-attack behaviors online. In his study of the social media postings and private communications of the right-wing Norwegian extremist Anders Behring Breivik, he contends that little meaningful insight can be gleaned (Ravndal 2013). Indeed, the state “security authorities would likely not react to [Breivik’s] online postings even if he was being monitored” (Ravndal 2013).

#### 4.2 Network Mapping

Not all studies of online extremism at the level of the user focus on terrorist propaganda and logistics. Expanding our qualitative understanding of how extremist communities operate collectively online are Conway, whose research into what constitutes a “radical milieu” offers a useful explainer of the complex social dynamics that give rise to them, and Prucha, whose work attempts to navigate through what he calls the “online territories of terror” (Conway 2012; Prucha 2011). Both Conway and Prucha contend that these virtual terrains are home to a rich spectrum of informal activism and cultural exchange, something that is captured vividly in Amarasingam’s brief account of IS’s online “family” (Amarasingam 2015). Koehler, whose research focuses on how right-wing extremists use online spaces, comes to a similar conclusion: the Internet, he holds, is home to a “plurality” of ideological interactions and forms of social engagement (Koehler 2015). These findings are reiterated in the accounts of Bowman-Grieve, De Koster and Houtman, and Caren, Jowers, and Gaby, each of which also explores the far-right online through the lens of the “Stormfront” forum (Bowman-Grieve 2009; De Koster and Houtman 2008; Caren, Jowers, and Gaby 2012). Echoing Amarasingam, Bowman-Grieve holds that “virtual communities are real social spaces” that can-

not simply be unpicked from offline extremist activism, something also found by De Koster and Houtman in their examination of the virtual “sense of community” proffered by the website’s users (Bowman-Grieve 2009, 990; De Koster and Houtman 2008). Besides these works, not to mention Conway and McInierney’s and al-Shishani’s examinations of jihadist extremism on YouTube and Facebook, there are relatively few other examples of qualitative research into extremist networks at the user level (Conway and McInierney 2008; al-Shishani 2010).

By way of contrast, quantitative studies abound. Two of the earliest and most effective attempts to comprehensively map out online extremist networks – in this case, those related to the Syrian war – are the accounts of Carter et al. and Klausen (Carter, Maher, and Neumann 2014; Klausen 2014). Berger’s 2015 and 2016 contributions on the topic, the first of which maps IS networks on Twitter and the second of which compares them with those of white nationalists in the United States, provide among the most comprehensive accounts of jihadist social networks on Twitter (Berger 2016). His and Perez’s analysis, published seven months later, identifies “huge declines in virtually every social media success metric” for supporters of the self-proclaimed caliphate (Berger and Perez 2016, 17). Concurrently, they note that white nationalist extremism has never posed a more substantial threat online: indeed, accounts linked to it “outperform ISIS in nearly every social metric, from follower counts to tweets per day” (Berger 2016, 3). Alexander comes to a similar conclusion, albeit with less confidence of success in the social media war against IS supporters (Alexander 2017).

Also evaluating the online performance of IS, Awan examines a small number of Facebook and Twitter accounts with a view to developing a behavioral typology for the group’s supporters (Awan 2017). While it makes for an interesting methodological approach, the resultant analysis is somewhat over-generalized: he concludes that “propaganda, recruitment and radicalization” are the three key characteristics of IS’s online extremism (Awan 2017, 147). Notwithstanding this, Awan does make a crucial observation that is all too often ignored: that not all those engaging in virtual support of the organization would ever take their

activism into the real world. Indeed, he notes, it is often the case that these communities comprise individuals “seeking an adrenaline rush [and] looking for excitement” online, and nothing more (Awan 2017, 148).

In any case, whether the approach is quantitative or qualitative, a conclusion regularly drawn by researchers into virtual extremist communities is that they cannot be generalized. While there may be recurrent trends and dynamics, there are no universal structures or systems, and, considering this, any academic enquiry must take an atomized approach towards understanding them, segmenting different spheres of activity, and ideology.

### 4.3 Women’s Participation

A final thematic cluster in the literature relates to women’s engagement and participation in extremism online. While scholars have long studied gender dynamics in the context of extremism and terrorism, relatively few explored how female extremists use online spaces prior to 2014. Since then, though, analysts and scholars have made many useful contributions. On the specific issue of how social media platforms are integrated into IS’s recruitment of women, the Institute for Strategic Dialogue has published two helpful investigations (Hoyle, Bradford, and Frenett 2015; Saltman and Smith 2015). However, while based on empirical observations, the datasets are relatively small and the resultant analysis mostly descriptive. Besides these reports, articles by Pearson, Manrique et al., and Huey and Peladeau stand out. Pearson’s account of Roshonara Choudhry’s online interactions prior to her attempted killing of British Member of Parliament Stephen Timms offers systematic analysis of the failed assassin’s seemingly anomalous experience of radicalization (Pearson 2015). For their part, Manrique et al. study community network dynamics among female IS sympathizers on VKontakte and Facebook, demonstrating the surprising extent of their activism, while Huey and Peladeau, whose comparative study is also based on a robust multi-platform dataset, examine a different aspect of the issue, positing that the role of women as online cheerleaders for jihadist violence constitutes a qualitative shift in the nature of gendered extremism (Manrique et al. 2016; Huey and Peladeau 2016).

## 5 Countering Extremism Online

As policymakers honed their strategies for tackling online extremism over the course of the last decade, the academic literature on what works and what does not has swelled. Broadly speaking, it can be divided into analyses of defensive, or reactive, measures, and analyses of offensive, or proactive, measures.

### 5.1 Reactive Means

Regarding the first, scholars have long held that countering online extremism requires a comprehensive, whole-of-society response. Two of the first to meaningfully examine this idea are Weimann and von Knop, who discuss the notion of “noise” in the context of challenging extremist strategic communication operations (Weimann and von Knop 2008). Specifically, they identify five “key elements” that should be prioritized in developing a counter-strategy: socio-political and theological credibility, knowledge of the appropriate terminology, awareness of cultural traditions, the presence of multiple partners, and the development of a global outlook (Weimann and von Knop 2008, 891). Neumann and Stevens call for a similar set of tools in their proposed strategy for countering online extremism, which combines negative measures – i.e., censorship and account suspension – with crowd-sourced counter-activism (Stevens and Neumann 2012). Neumann returns to these ideas in the specific context of countering online extremism in the United States, noting that governments are duty-bound to encourage civic challenges to extremism while also promoting awareness and education (Neumann 2013b).

The need for counter-strategic communication campaigns to have a high degree of quality, flexibility, and credibility frequently emerges in the literature. As Bean and Edgar note, if the adversary’s message is inherently more appealing because of the skill with which it is constructed, simplistic and “sterile” attempts at countering it are bound to failure (Bean and Edgar 2017, 329). Echoing this, McDowell-Smith et al. found that American students considered carefully curated defector interview videos “authentic, disturbing and [likely to] turn them away from ISIS” (McDowell-Smith, Speckhard, and Yayla 2017). For counter-strategic communication campaigns content to be impactful, then, it seems that credibility is key.

That being said, as Archetti notes, it is not enough to simply will individuals to act in a given way: “persuasion to think and act in a way desired by the originator of a message cannot be simply inferred from the content of the communication” (Archetti 2018, 9). This is especially the case if said originator is already regarded as an illegitimate broker. If, say, McDowell-Smith, Speckhard, and Yayla’s study were to be repeated with focus groups containing young people from northern Iraq, it would almost certainly return different results.

Besides these accounts, there have been several investigations into the feasibility and effectiveness of hard defensive policies in the sense of negative measures. Since 2014, governments have exerted strong pressure on private companies to aggressively undermine the extremist networks present on their platforms, chiefly through account suspensions and the censorship of propaganda (Fioretti 2017). Berger and Milton’s works tracking corporate efforts in response to this pressure are particularly influential, and are complemented by Conway et al., who come to a similar conclusion (Conway et al. 2017). However, not all accounts have found that aggressive negative measures have “worked.” Besides Alexander’s argument that the “fight against IS on Twitter is far from over,” Pearson, writing about the psychological impact of account censorship, notes that such suspensions had become an “integral” part of the online identities of pro-IS extremists (Pearson 2015). An even more ardent critic of negative measures is Fisher, who has long held that they are being insufficiently implemented. In a 2017 report, he claims that there has been no meaningful drop in either the number of pro-IS users or the volume of propaganda, and calls for governments to put even more pressure on Internet companies (Frampton, Fisher, and Prucha 2017). Klein and Flinn offer a similar set of recommendations, contending that it is within the legislative rights of governments to force social media corporations to comply with their counter-terrorism policy objectives (Klein and Flinn 2017). Besides these two accounts, it is worth noting that few other researchers have come to this conclusion.

## 5.2 Proactive Measures

In terms of offensive attempts to counter extremism online, the literature is split into two: that which focuses on the narrative space, and that which pertains to security. In regard to the former, there have been a large number of ideas-focused studies conducted by think-tanks, which emphasize the need for a positive foundation – in their words, an alternative narrative – to counter-strategic communication campaigns (Silverman et al. 2016; Tuck and Silverman 2016; Briggs and Feve 2014; Reynolds and Scott 2016; Bartlett and Krasomdomski-Jones 2016). These works repeatedly note that counter-messaging must be more aggressive – that is, it must do more than point out negative characteristics of the adversary. Ingram’s linkage-based strategy for engaging in communication counter-strategies gives theoretical legs to this idea (Ingram 2016a). He recommends that campaigns should undermine extremist narratives by dismantling the “systems of meaning” that undergird them, while also using network disruption strategies to “trigger behavioral changes away from support” for extremism (Ingram 2016a, 11).

Seeking to better inform the kind of offensive information campaigns that scholars like Ingram are calling for, the Atlanta-based Carter Center published an edited volume, focusing on how IS can be challenged through theological argumentation (Carter Center 2016). Al-Saud, examines this issue from a similar angle in a detailed case study of the Saudi Arabia-based Sakinah Campaign, an online initiative that started out as a primarily defensive communications program but that moved, with time, to adopt a more proactive, offensive narrative stance (Al-Saud 2017). While her focus is also on offensive counter-strategic communication, Johanson’s work evaluates the impact of a vastly different example, the “ISIS-Chan” meme. This is a Manga cartoon that was used in early 2015 to ridicule IS on Twitter, obstruct its propaganda operations, and degrade its status as a credible communicator (Johanson 2017).

Lastly, scholars have undertaken many data-informed investigations. While most of these studies have focused on Twitter, which, as discussed, is generally the easiest to access in terms of data analytics, Diaz et al. (2016) take an algorithmic approach to

wards understanding and locating extremist dynamics on forums, as do Scrivens, Davies, and Frank, who use linguistic analysis to identify nascent and confirmed instances of radicalization in non-extremist Islamic forums (Scrivens, Davies, and Frank 2016). Attempting to develop a similar sentiment-based detection system among English-speakers on YouTube, Bermingham et al. note that the approach has potential, notwithstanding its large number of potential pitfalls (Bermingham et al. 2009). Using a similar sentiment analysis-based approach, Magdy, Darwish, and Weber use Twitter analytics to longitudinally track the hardening of ideological positions among Arabic-speakers (Magdy, Darwish, and Weber 2015). In so doing, they capture the transition of individuals from expressing feelings of ambivalence towards jihadism to expressing overt support of it, which they see as a response to the failure of the Arab Spring. Saif et al. also develop a semantic approach towards detecting “signs of radicalization” among Twitter users (Saif et al. 2017). Like Magdy, Darwish, and Weber, they conclude that moderate benefits can be gleaned from using social media in this way, but that algorithmic techniques alone are an imperfect measure of radicalization. For their part, Riebe et al.’s 2018 contribution uses quantitative content analysis to track discourse shifts in the Facebook posts of supporters of the right-wing German Alternative für Deutschland party, thereby finetuning similar efforts at using social media data to detect and assess extremist tendencies online. While none of these studies attempt to identify a definitive set of signifiers for the (potential) presence of extremism and/or radicalization, they all highlight that semantic and linguistic analysis, if used as part of a package of intelligence-gathering measures, have great potential.

## 6 Conclusions, Policy Options, and Avenues for Further Research

Online extremism has never received as much attention from academics as it does today. The literature is diverse and wide-ranging, and, especially since the early 2010s, increasingly scientific. From network-mapping to sentiment analyses and impact assessments of propaganda consumption, scholars are increasingly incorporating small- and large-N datasets

into their work. Such quantitative rigor is sorely needed. However, this emergent preference for quantitative methods risks coming at the expensive of insights that can only be derived from qualitative exploration. In any case, scholars would do well to continue developing and implementing innovative mixed-methods research designs, for, even in this crowded marketplace, academic inquiry can still produce many tangible social and security benefits.

Broadly speaking, two key points of consensus emerge from the literature. First, scholars generally seem to agree that “online extremism” often amounts to nothing more than orthodox usage of the Internet that is as intuitive as it is innovative. Indeed, while it is undoubtedly true that extremists make extensive use of online spaces, the literature suggests that – with a few exceptions – they rarely do it in a way that is particularly revolutionary. The second point of consensus is that it makes little sense to attempt to counter extremism online without concurrently seeking to understand and challenge its offline manifestations. While policymakers still tend to neatly separate the online and offline spheres, two decades’ worth of academic inquiry has demonstrated, fairly resolutely, that such a separation cannot – and, if policy is to work, must not – be made.

The literature review reveals areas for further investigation as well as policy recommendations, particularly on the currently most important debates in the field: Is it still meaningful to speak of online radicalization and online extremism? What is the connection between online hate speech and violence? To what extent do different extremist groups have similar ways of operating online? What exactly influences the interplay of online and offline factors when it comes to radicalization? Is the removal of extremist publications from the Internet an effective measure for countering extremism? Do narrative and counter-narratives work? How does encrypted communication, especially on messaging platforms, influence online radicalization (if it does at all)?

One of the greatest challenges is certainly the rapidly changing technological landscape. Research conducted today will likely have been overtaken by technical developments by the time it is published in two or three years. As a result, researchers must ask

themselves which questions they can most meaningfully study in this context, and how they can better cooperate with practitioners, particularly in the field of technology.

Further, researchers should become more effectively involved in public debates based on their empirical knowledge and participate on topics such as censorship and Internet regulation. Governments regularly demand that extremist retreats on the Internet should be removed, without fully understanding the intricacies of online extremism, or how effective such measures really are. It is important that academics contribute to those resolutions, independent of the important ethical and philosophical questions that arise as a result.

## References

- Abay Gaspar, Hande, Christopher Daase, Nicole Deitelhoff, Julian Junk, and Manjana Sold. 2020. Radicalization and Political Violence: Challenges of Conceptualizing and Researching Origins, Processes and Politics of Illiberal Beliefs. *International Journal for Conflict and Violence*. 14 (2): 1-18. doi:10.4119/ijcv-3802.
- Adelman, Rebecca R. 2018. One Apostate Run Over, Hundreds Repented: Excess, Unthinkability, and Infographics from the War with I.S.I.S. *Critical Studies in Media Communication* 35 (1): 57–73.
- Aggarwal, Neil Krishan. 2016. *The Taliban's Virtual Emirate: The Culture and Psychology of an Online Militant Community*. New York: Columbia University Press.
- Alexander, Audrey. 2017. *Digital Decay: Tracing Change Over Time among English-Language Islamic State Sympathizers on Twitter*. Washington, D.C.: George Washington University Program on Extremism. [https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal\\_0.pdf](https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf).
- Al-Rawi, Ahmed. 2016. Video Games, Terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence* 30 (4): 740–60. <http://www.tandfonline.com/doi/full/10.1080/09546553.2016.1207633>.
- Al-Saud, Abdullah bin Khaled. 2017. The Tranquillity Campaign: A Beacon of Light in the Dark World Wide Web. *Perspectives on Terrorism* 11 (2): 58–64.
- Al-Shishani, Murad Batal. 2010. Taking Al-Qaeda's Jihad to Facebook. *Jamestown Terrorism Monitor* 5 (4): 3–4.
- Amarasingam, Amarnath. 2015. Elton "Ibrahim" Simpson's Path to Jihad in Garland, Texas. *War on the Rocks*, May 14. <https://warontherocks.com/2015/05/elton-ibrahim-simpsons-path-to-jihad-in-garland-texas/>.
- Anzalone, Christopher. 2010. From "Martyrdom" Videos to Jihadi Journalism in Somalia. *Informed Comment*, 25 August. <https://www.juancole.com/2010/08/anzalone-from-%E2%80%98martyrdom%E2%80%99-videos-to-jihadi-journalism-in-somalia.html>.
- Anzalone, Christopher. 2016. Continuity and Change: The Evolution and Resilience of Al-Shabab's Media Insurgency, 2006–2016. *Hate Speech International*, 9 November. <https://www.hate-speech.org/new-report-on-al-shabab-media/>.
- Archetti, Christina. 2013. *Understanding Terrorism in the Age of Global Media: A Communication Approach*. New York: Palgrave Macmillan.
- Archetti, Christina. 2018. The Unbearable Thinness of Strategic Communication. In *Countering Online Propaganda and Violent Extremism: The Dark Side of Digital Diplomacy*, ed. Comeliu Bjola and James Pamment, 81–96. Abingdon-on-Thames: Routledge.
- Atton, Christina. 2006. Far-Right Media on the Internet: Culture, Discourse and Power. *New Media and Society* 8 (4): 573–87.
- Awan, Imran. 2017. Cyber-Extremism: Isis and the Power of Social Media. *Society* 54 (2): 138–49.
- Bartlett, Jamie, and Alex Krasomdomski-Jones. 2016. *Counter-speech on Facebook*. London: DEMOS. <https://www.Demos.co.uk/wp-content/uploads/2016/09/Counter-speech-on-facebook-report.pdf>.
- Bean, Hamilton, and Amanda Edgar. 2017. A Genosonic Analysis of ISIL and US Counter-Extremism Video Messages. *Media, War, and Conflict* 10 (3): 327–44.
- Benson, David C. 2014. Why the Internet Is Not Increasing Terrorism. *Security Studies* 23 (2): 293–328.
- Bergen, Peter. 2016. *ISIS Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media. [Prepared testimony]*. Washington, DC: Committee on Homeland Security. [https://www.hsgac.senate.gov/download/bergen-testimony\\_psi-2016-07-05](https://www.hsgac.senate.gov/download/bergen-testimony_psi-2016-07-05).
- Bergen, Peter, Bruce Hoffmann, Michael Hurley, and Erroll Suthers. 2013. *Jihadist Terrorism: A Threat Assessment*. Washington, DC: Bipartisan Policy Centre.
- Berger, J. M. 2015. How Terrorists Recruit Online (and How to Stop It). Brookings Institution, Markaz blog, 9 November. <https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/>.
- Berger, J. M. 2016. *Nazis vs. ISIS on Twitter: A Comparative Study of White Nationalist and ISIS Online Social Media Networks*. Washington, DC: George Washington University Program on Extremism. [https://cchs.gwu.edu/files/downloads/Nazis%2520v.%2520ISIS%2520Final\\_0.pdf](https://cchs.gwu.edu/files/downloads/Nazis%2520v.%2520ISIS%2520Final_0.pdf).
- Berger, J. M. 2017. *Deconstruction of Identity Concepts in Islamic State Propaganda: A Linkage-Based Approach to Counter-Terrorism Strategic Communications*. The Hague: EUROPOL. [https://icct.nl/wp-content/uploads/2017/06/bergerjm\\_deconstructionofislamicstatetexts.pdf](https://icct.nl/wp-content/uploads/2017/06/bergerjm_deconstructionofislamicstatetexts.pdf).
- Berger, J. M., and Jonathon Morgan. 2015. *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*. Washington, DC: Brookings Institution. [https://www.brookings.edu/wp-content/uploads/2016/06/isis\\_twitter\\_census\\_berger\\_morgan.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf).
- Berger, J. M., and Heather Perez. 2016. *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters*. Washington, DC: George Washington University Program on Extremism. <https://cchs.gwu.edu/sites/cch>



- s.gwu.edu/files/downloads/Berger\_Occasional%20Paper-pdf.
- Berger, J. M., and Jessica Stern. 2015. *ISIS: The State of Terror*. New York: HarperCollins.
- Birmingham, Adam, Maura Conway, Lisa McInerney, Neil O'Hare, and Alan Smeaton. 2009. Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation: In *Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining*, 231–36. <http://doras.dcu.ie/4554/>.
- Bloom, Mia, Hicham Tiflati, and John Horgan. 2017. Navigating ISIS's Preferred Platform: Telegram. *Terrorism and Political Violence*, July, 1–13. <http://www.tandfonline.com/doi/full/10.1080/09546553.2017.1339695>.
- Bonafante, Luigi. 1979. Some Unanticipated Consequences of Terrorism. *Journal of Peace Research* 3 (16): 197–211.
- Bowman-Grieve, Lorraine. 2009. Exploring “Stormfront”: A Virtual Community of the Radical Right. *Studies in Conflict and Terrorism* 32 (11): 989–1007.
- Brantly, Aaron. 2017. Banning Encryption to Stop Terrorists: A Worse Than Futile Exercise. *Combating Terrorism Center Sentinel* 10 (5): 29–33.
- Briggs, Rachel, and Sebastien Feve. 2014. *Counter the Appeal of Extremism Online*. London: Institute for Strategic Dialogue. <https://www.dhs.gov/sites/default/files/publications/Countering%20the%20Appeal%20of%20Extremism%20Online-ISR%20Report.pdf>.
- Burris, Val, Eemery Smith, and Ann Strahm. 2000. White Supremacist Networks on the Internet. *Sociological Focus* 33 (2): 215–35.
- Callimachi, Rukmini. 2015. ISIS and the Lonely Young American. *New York Times*, 27 June. <https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html>.
- Callimachi, Rukmini. 2017. Not “Lone Wolves” After All: How ISIS Guides World's Terror Plots from Afar. *New York Times*, 4 February. <https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html>.
- Camstoll Group. 2016. *Use of Social Media by Terrorist Fundraisers and Financiers*. Los Angeles and Washington, D.C.: Camstoll Group. <https://www.camstoll.com/wp-content/uploads/2016/04/Social-Media-Report-4.22.16.pdf>.
- Caren, Neal, Kay Jowers, and Sarah Gaby. 2012. A Social Movement Online Community: Stormfront and the White Nationalist Movement. In *Media, Movements, and Political Change*, ed. Jennifer Earl and Deana A. Rohlinger, 163–93. Bingley, UK: Emerald Group.
- Carter, Joseph A., Shiraz Maher, and Peter R. Neumann. 2014. #Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks. London: International Centre for the Study of Radicalisation. <https://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Influence-in-Syrian-Foreign-Fighter-Networks.pdf>.
- Carter Center. 2016. *Countering Daesh Propaganda: Action-Oriented Research for Practical Policy Outcomes*. Atlanta, GA: Carter Center. [https://www.cartercenter.org/re-sources/pdfs/peace/conflict\\_resolution/countering-isis/counteringdaeshpropaganda-feb2016.pdf](https://www.cartercenter.org/re-sources/pdfs/peace/conflict_resolution/countering-isis/counteringdaeshpropaganda-feb2016.pdf).
- Chouliaraki, Lilie, and Angelos Kissas. 2017. The Communication of Horrorism: A Typology of ISIS Online Death Videos. *Critical Studies in Media Communication* 35 (1): 24–39.
- Conway, Maura. 2005. Terrorist Web Sites: Their Contents, Functioning, and Effectiveness. In *New Media and the New Middle East*, ed. Philip Seib, 235–58. New York: Palgrave Macmillan.
- Conway, Maura. 2012. From Al-Zarqawi to Al-Awlaki: The Emergence and Development of an Online Radical Milieu. *CTX: Combating Terrorism Exchange* 2 (4): 12–22.
- Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weir. 2017. *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts*. N.p.: VOX-Pol. [http://www.voxpol.eu/download/vox-pol\\_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf](http://www.voxpol.eu/download/vox-pol_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf).
- Conway, Maura, and Lisa McInerney. 2008. Jihadi Video and Auto-Radicalisation: Evidence from an Exploratory Youtube Study. In *Intelligence and Security Informatics*, ed. Daniel Ortiz-Arroyo, Henrik Legind Larsen, Daniel Dajun Zeng, David Hicks, and Gerhard Wagner, 108–18. Esbjerg: EuroISI.
- De Koster, Willem, and Dick Houtman. 2008. “Stormfront Is Like a Second Home to Me”: On Virtual Community Formation by Right-Wing Extremists. *Information, Communication and Society* 11 (8): 1155–76.
- della Porta, Donatella, and Gary LaFree. 2012. Processes of Radicalization and De-Radicalization. *International Journal of Conflict and Violence* 6 (1): 4–10.
- Diaz, Alexandro R., Jongeun Choi, Thomas J. Holt, Steven Chermak, and Joshua D. Freilich. 2016. Data-driven System Identification of the Social Network Dynamics in Online Postings of an Extremist Group. In *2016 IEEE International Conference on Cybercrime and Computer Forensic*, ed. Barry Cartwright, George Weir and Laurie Yiu-Chung Lau, n.p. N.p.: IEEE.
- Donelan, Helen. 2009. *Online Communication and Collaboration: A Reader*. Abingdon-on-Thames: Routledge.
- Douglas, Karen, Graig McGarty, Ana-Maria Bliuc, and Girish Lala. 2005. Understanding Cyberhate: Social Competition and Social Creativity in Online White Supremacist Groups. *Social Science Computer Review* 23 (1): 68–76.
- Farwell, James P. 2014. The Media Strategy of ISIS. *Survival* 56 (6): 49–55.
- Feuer, Alan. 2018. One Brooklyn Man's Lonely Journey to Jihad. *New York Times*, 3 January. <https://www.nytimes.com/2018/01/03/nyregion/akhror-saidakhmetov-terror-brooklyn-nyc.html>.
- Fioretti, Julia. 2017. Social Media Giants Step Up to Join Fight Against Extremist Content. Reuters, 26 June. <https://www.reuters.com/article/us-internet-extremism/social-media-giants-step-up-joint-fight-against-extremist-content-idUSKBN19H20A>.
- Frampton, Martyn, Ali Fisher, and Nico Prucha. 2017. *The New Netwar: Countering Extremism Online*. London: Policy Exchange. <https://policyexchange.org.uk/wp-content/uploads/2017/09/The-New-Netwar-1.pdf>.

- Freiburger, Tina, and Jeffrey Crane. 2008. A Systematic Examination of Terrorist Use of the Internet. *International Journal of Cyber Criminology* 2 (1): 309–19.
- Gambhir, Harleen. 2016. *The Virtual Caliphate: ISIS's Information Warfare*. Washington, DC: Institute for the Study of War. <http://www.understandingwar.org/backgrounders/virtual-caliphate-isiss-information-warfare>.
- Gartenstein-Ross, Daveed, and Nathaniel Barr. 2016. The Myth of Lone-Wolf Terrorism. *Foreign Affairs*. <http://www.defenddemocracy.org/media-hit/gartenstein-ross-daveed-the-myth-of-lone-wolf-terrorism/>.
- Gartenstein-Ross, Daveed, Nathaniel Barr, and Bridget Moreng. 2016. *The Islamic State's Global Propaganda Strategy*. The Hague: International Centre for Counter-Terrorism. <https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Gartenstein-Ross-IS-Global-Propaganda-Strategy-March2016.pdf>.
- Gartenstein-Ross, Daveed, and Madeleine Blackman. 2017. ISIL's Virtual Planners: A Critical Terrorist Innovation. *War on the Rocks*, 4 January. <https://warontherocks.com/2017/01/isils-virtual-planners-a-critical-terrorist-innovation/>.
- Gates, Scott, and Sukanya Podder. 2015. Social Media, Recruitment, Allegiance and the Islamic State. *Perspectives on Terrorism* 9 (4): 107–16. <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/446>.
- Geeraerts, Sanne B. 2012. Digital Radicalization of Youth. *Social Cosmos* 3 (1): 25–32.
- Gendron, Angela. 2017. The Call to Jihad: Charismatic Preachers and the Internet. *Studies in Conflict and Terrorism* 40 (1): 44–61.
- Gerstenfeld, Phyllis B., Diana R. Grant, and Chau-Pu Chiang. 2003. Hate Online: A Content Analysis of Extremist Internet Sites. *Analyses of Social Issues and Public Policy* 3 (1): 29–44.
- Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. Terrorist Use of the Internet by the Numbers: Quantifying Behaviours, Patterns, and Processes. *Criminology and Public Policy* 16 (1): 99–117.
- Gill, Paul, John Horgan, and Paige Deckert. 2014. Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. *Journal of Forensic Sciences* 59 (2): 425–35.
- Goldman, Zachary K., Elli Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. 2017. *Terrorist Use of Virtual Currencies: Containing the Potential Threat*. Washington, DC: CNAS. <http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf>.
- Hegghammer, Thomas. n.d. *Interpersonal Trust on Jihadi Internet Forums*. Unpublished manuscript.
- Hoffman, Bruce. 2006. *Using the Web as a Weapon: The Internet as a Tool for Violent Radicalization and Homegrown Terrorism. [Prepared Testimony]*. Washington, DC: Committee on Homeland Security. [https://fas.org/irp/congress/2007\\_hr/web.pdf](https://fas.org/irp/congress/2007_hr/web.pdf).
- Hoffman, Bruce. 2008. The Myth of Grass-Roots Terrorism: Why Osama bin Laden Still Matters. *Foreign Affairs* 87 (3): 133–38.
- Hoffman, Bruce. 2017. *Inside Terrorism*. New York: Columbia University Press.
- Holbrook, Donald. 2013. Far Right and Islamist Extremist Discourses: Shifting Patterns of Enmity. In *Extreme Right Wing Political Violence and Terrorism*, ed. Max Taylor, P. M. Currie, and Donald Holbrook, 215–37. London: Bloomsbury Academic.
- Holbrook, Donald. 2015. A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acts of Terrorism. *Dynamics of Asymmetric Conflict* 8 (2): 121–33.
- Holbrook, Donald. 2017. *What Types of Media Do Terrorists Collect? An Analysis of Religious, Political, and Ideological Publications Found in Terrorism Investigations in the UK*. The Hague: International Centre for Counter-Terrorism. <https://icct.nl/wp-content/uploads/2017/09/ICCT-Holbrook-What-Types-of-Media-Do-Terrorists-Collect-Sept-2017-2.pdf>.
- Hoskins, Andrew, and Ben O'Loughlin. 2009. Media and the Myth of Radicalisation. *Media, War, and Conflict* 2 (2): 107–10.
- Hoyle, Carolyn, Alexandra Bradford, and Ross Frenett. 2015. *Becoming Mulan? Female Western Migrants to ISIS*. London: Institute for Strategic Dialogue. [https://www.isdglobal.org/wp-content/uploads/2016/02/ISDJ2969\\_Becoming\\_Mulan\\_01.15\\_WEB.pdf](https://www.isdglobal.org/wp-content/uploads/2016/02/ISDJ2969_Becoming_Mulan_01.15_WEB.pdf).
- Huey, Laura, and Hillary Peladeau. 2016. *Cheering on the Jihad: An Exploration of Women's Participation in Online Pro-Jihadist Networks*. Waterloo, Ontario: The Canadian Network for Research on Terrorism, Security and Society. [http://tsas.ca/wp-content/uploads/2016/05/TSASWP16-07\\_Huey-Peladeau.pdf](http://tsas.ca/wp-content/uploads/2016/05/TSASWP16-07_Huey-Peladeau.pdf).
- Hughes, Seamus, and Alexander Meleagrou-Hitchens. 2017. The Threat to the United States from the Islamic State's Virtual Entrepreneurs. *Combating Terrorism Center Sentinel* 10 (31): 1–8.
- Iannaccone, Laurence, and Eli Berman. 2006. Religious Extremism: The Good, The Bad, and the Deadly. *Public Choice* 128 (1): 109–29.
- Ingram, Haroro J.. 2015. The Strategic Logic of Islamic State Information Operations. *Australian Journal of International Affairs* 69 (6): 729–52.
- Ingram, Haroro J. 2016a. *A "Linkage-Based" Approach to Combating Militant Islamist Propaganda: A Two-Tiered Framework for Practitioners*. The Hague: International Centre for Counter-Terrorism. <https://icct.nl/wp-content/uploads/2016/11/ICCT-Ingram-A-Linkage-Based-Approach-Nov2016.pdf>.
- Ingram, Haroro J. 2016b. An Analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State's Propaganda War. *Studies in Conflict & Terrorism* 40 (5): 357–375.
- Ingram, Haroro J., and Craig Whiteside. 2017. The Yemen Raid and the Ghost of Anwar al-Awlaki. *Atlantic*, 9 February. <https://www.theatlantic.com/international/archive/2017/02/yemen-raid-trump-awlaki-al-qaeda-isis/516180/>.
- Jacobson, Michael. 2009. Terrorist Financing on the Internet. *Combating Terrorism Center Sentinel* 2 (6): 17–20. <https://www.washingtoninstitute.org/uploads/Documents/opeds/4a438817e3a3c.pdf>.
- Johanson, Anna. 2017. ISIS-Chan – The Meanings of the Manga Girl in Image Warfare Against the Islamic State.

- Critical Studies on Terrorism* 11 (1): 1–25. <http://www.tandfonline.com/doi/full/10.1080/17539153-2017.1348889?scroll=top&needAccess=true>.
- Johnson, Neil, Minzhang Zheng, Yulia Vorobyeva, Andrew Gabriel, Houliang Qi, Nicolas Velasquez, Pedro Manrique, Darnell Johnson, Eduardo Restrepo, Chaoming Song, and Stefan Wuchty. 2016. New Online Ecology of Adversarial Aggregates: ISIS and Beyond. *Science* 352 (6292): 1459–63.
- Kamolnick, Paul. 2017. How Muslim Defenders Became “Blood Spilling” Crusaders: Adam Gadahn’s Critique of the “Jihadist” Subversion of Al Qaeda’s Media Warfare Strategy. *Terrorism and Political Violence* 29 (3): 444–63.
- Katz, Rita. 2016. Almost Any Messaging App Will Do – If You’re ISIS. *Vice Motherboard*, July 14. [https://motherboard.vice.com/en\\_us/article/kb7n4a/isis-messaging-apps](https://motherboard.vice.com/en_us/article/kb7n4a/isis-messaging-apps).
- Kenney, Michael. 2010. Beyond the Internet: Metis, Techne and the Limitations of Online Artifacts for Islamist Terrorists. *Terrorism and Political Violence* 22 (2): 177–97.
- Khatib, Lina. 2013. *Image Politics in the Middle East: The Role of the Visual in Political Struggle*. London: I. B. Tauris.
- Kimmage, Daniel. 2008. *The Al-Qaeda Media Nexus*. Washington, DC: Radio Free Europe Radio Liberty. [https://docs.rferl.org/en-US/AQ\\_Media\\_Nexus.pdf](https://docs.rferl.org/en-US/AQ_Media_Nexus.pdf).
- Kimmage, Daniel. 2010. *Al-Qaeda Central and the Internet*. Washington, DC: New America Foundation. [https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HSPI\\_Report\\_15.pdf](https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HSPI_Report_15.pdf).
- Klausen, Jytte. 2015. Tweeting the Jihad. *Studies in Conflict and Terrorism* 38 (1): 1–22.
- Klein, Susan, and Crystal Flinn. 2017. Social Media Compliance Programs and the War against Terrorism. *Harvard National Security Journal* 8: 53–112.
- Koehler, Daniel. 2015. The Radical Online: Individual Radicalization Processes and the Role of the Internet. *Journal for Deradicalization* 1 (winter 2014/15): 116–34.
- Lia, Brynjar, and Thomas Hegghammer. 2010. Jihadi Strategic Studies: The Alleged Al Qaida Policy Study Preceding the Madrid Bombings. *Studies in Conflict and Terrorism* 27 (5): 355–75.
- Magdy, Walid, Kareem Darwish, and Ingmar Weber. 2015. *#Failedrevolutions: Using Twitter to Study the Antecedents of ISIS Support*. N.p.: Association for the Advancement of Artificial Intelligence. <https://arxiv.org/pdf/1503.02401.pdf>.
- Manrique, Pedro, Zhenfeng Cao, Andrew Gabriel, John Horgan, Paul Gill, Hong Qi, Elvira Restrepo, Daniela Johnson, Stefan Wuchty, Chaoming Song, and Neil Johnson. 2016. Women’s Connectivity in Extreme Networks. *Science Advances* 2 (6): e1501742. <http://advances.sciencemag.org/content/advances/2/6/e1501742.full.pdf>.
- Meleagrou-Hitchens, Alexander. 2012. *As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad*. London: International Centre for the Study of Radicalisation. <https://icsr.info/wp-content/uploads/2011/09/ICSR-Report-As-American-As-Apple-Pie-How-Anwar-al-Awlaki-Became-the-Face-of-Western-Jihad.pdf>.
- Meleagrou-Hitchens, Alexander, and Nick Kaderbhai. 2017. *Research Perspectives on Online Radicalisation: A Literature Review, 2006–2016*. N.p.: VOX-Pol. <http://icsr.info/2017/05/icsr-vox-pol-paper-research-perspectives-online-radicalisation-literature-review-2006-2016/>.
- McCauley, Clark, and Sophia Moskalenko. 2008. Mechanisms of Political Radicalization: Pathways toward Terrorism. *Terrorism and Political Violence* 20 (3): 415–33.
- McDowell-Smith, Allison, Anne Speckhard, and Ahmet S. Yayla. 2017. Beating ISIS in the Digital Space: Focus Testing ISIS Defector Counter-Narrative Videos with American College Students. *Journal for Deradicalization* 1 (10). <http://journals.sfu.ca/jd/index.php/jd/article/view/83>.
- Milton, Daniel. 2016. *Communication Breakdown: Unravelling the Islamic State’s Media Efforts*. West Point: Combating Terrorism Center.
- Mozes, Tomer, and Gabriel Weimann. 2010. The E-Marketing Strategy of Hamas. *Studies in Conflict and Terrorism* 33 (3): 211–25.
- Neumann, Peter. 2013a. Radikalisierung, Deradikalisierung und Extremismus. *Aus Politik und Zeitgeschichte* 63: 3–10.
- Neumann, Peter. 2013b. Options and Strategies for Countering Online Radicalization in the United States. *Studies in Conflict and Terrorism* 36 (6): 431–59.
- Neumann, Peter. 2013c. The Trouble with Radicalization. *International Affairs* 89 (4): 873–93.
- Neumann, Peter, and Brooke Rogers. 2011. *Recruitment and Mobilisation for the Islamist Militant Movement in Europe*. London: International Centre for the Study of Radicalisation. <http://icsr.info/2008/10/recruitment-and-mobilisation-for-the-islamist-militant-movement-in-europe/>.
- O’Halloran, Kay, Sabine Tan, Peter Wignell, John Bateman, Ducson Pham, Michele Grossman, and Andrew Vande Moere. 2016. Interpreting Text and Image Relations in Violent Extremist Discourse: A Mixed Methods Approach for Big Data Analytics. *Terrorism and Political Violence* 31 (3): 454–74. <http://www.tandfonline.com/doi/pdf/10.1080/09546553.2016.1233871?needAccess=true>.
- O’Hara, Kieron, and David Stevens. 2015. Echo Chambers and Online Radicalism: Assessing the Internet’s Complicity in Violent Extremism. *Policy and Internet* 7 (4): 401–22.
- Pauwels, Lieven, and Nele Schils. 2016. Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives. *Terrorism and Political Violence* 28 (1): 1–29.
- Pearson, Elizabeth. 2015. The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad. *Policy and Internet* 8 (1): 5–34.
- Phillips, Vaughan. 2017. The Islamic State’s Strategy: Bureaucratizing the Apocalypse through Strategic Communication. *Studies in Conflict and Terrorism* 40 (9): 731–57.
- Prucha, Nico. 2011. Online Territories of Terror: Utilizing the Internet for Terrorist Endeavors. *Orient* 4 (1). [http://www.jihadica.com/wp-content/uploads/2013/04/Article\\_ORIENT\\_IV\\_NicoPrucha.pdf](http://www.jihadica.com/wp-content/uploads/2013/04/Article_ORIENT_IV_NicoPrucha.pdf).
- Prucha, Nico, and Ali Fisher. 2013. Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda. *Combating Terrorism Center Sentinel* 6 (2): 19–23.

- Prus, Robert. 2005. Terrorism, Tyranny, and Religious Extremism as Collective Activity: Beyond the Deviant, Psychological and Power Mystiques. *American Sociologist* 36: (1): 47–74.
- Ramsay, Gilbert. 2013. *Jihadi Culture on the World Wide Web*. London: Bloomsbury.
- Ravndal, Jacob Aasland. 2013. Anders Behring Breivik's Use of the Internet and Social Media. *Journal EXIT-Deutschland*, 2013, no. 2, 172–85. <http://journals.sfu.ca/jed/index.php/jex/article/view/28/0>.
- Reed, Alastair, and Haroro J. Ingram. 2017. *Exploring the Role of Instructional Material in AQAP's Inspire and ISIS's Rumiyah*. The Hague: Europol. <https://www.europol.europa.eu/publications-documents/exploring-role-of-instructional-material-in-aqaps-inspire-and-isis-rumiyah>.
- Reiger, Diana, Lary Frischlich, and Gary Bente. 2013. *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*. Munich: Luchterhand Literaturverlag.
- Renfer, Marc, and Henriette Haas. 2008. Systematic Analysis in Counterterrorism: Messages on an Islamist Internet-Forum. *International Journal of Intelligence and Counterintelligence* 21 (2): 314–36.
- Reynolds, Louis, and Ralph Scott. 2016. *Digital Citizens: Countering Extremism Online*. London: Demos. <https://www.Demos.co.uk/wp-content/uploads/2016/12/Digital-Citizenship-web.pdf>.
- Reynolds, Louis, and Mohammed Hafez. 2017. Social Network Analysis of German Foreign Fighters in Syria and Iraq. *Terrorism and Political Violence* 31 (4): 661–86. <http://www.tandfonline.com/doi/abs/10.1080/09546553.2016.1272456>.
- Riebe, Thea, Katja Patsch, Marc-Andre Kaufhold, and Christian Reuter. 2018. From Conspiracies to Insults: A Case Study of Radicalisation in Social Media Discourse. *Mensch und Computer 2018 – Workshopband*, 02.–05. September 2018, Dresden.
- Rogan, Hanna. 2006. *Jihadism Online: A Study of How Al-Qaida and Radical Islamist Groups Use the Internet for Terrorist Purposes*. Kjeller, Norway: Norwegian Defence Research Establishment.
- Rudner, Martin. 2016. “Electronic Jihad”: The Internet as Al Qaeda's Catalyst for Global Terror. *Studies in Conflict and Terrorism* 40 (1): 10–23.
- Sageman, Marc. 2004. *Understanding Jihadi Networks*. Philadelphia: University of Pennsylvania Press.
- Sageman, Marc. 2005. Understanding Jihadi Networks. *Strategic Insights* 4 (4): n.p.
- Sageman, Marc. 2008. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press.
- Saif, Hassan, Thomas Dickinson, Leon Kastler, Miriam Fernandez, and Harith Alani. 2017. A Semantic Graph-Based Approach for Radicalisation Detection on Social Media. *European Semantic Web Conference 2017: The Semantic Web*, ed. Eva Blomqvist, Diana Maynard, Aldo Gangemi et al. 571–87. Cham, Germany: Springer International. [https://link.springer.com/chapter/10.1007/978-3-319-58068-5\\_35](https://link.springer.com/chapter/10.1007/978-3-319-58068-5_35).
- Salami, Iwa. 2017. Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This? *Studies in Conflict & Terrorism* 41 (12): 968–89. <http://www.tandfonline.com/doi/pdf/10.1080/1057610X.2017.1365464?needAccess=true>.
- Saltman, Erin, and Melanie Smith. 2015. “Till Martyrdom Do Us Part”: Gender and the ISIS Phenomenon. London: Institute for Strategic Dialogue. [https://www.isdglobal.org/wp-content/uploads/2016/02/Till\\_Martyrdom\\_Do\\_Us\\_Part\\_Gender\\_and\\_the\\_ISIS\\_Phenomenon.pdf](https://www.isdglobal.org/wp-content/uploads/2016/02/Till_Martyrdom_Do_Us_Part_Gender_and_the_ISIS_Phenomenon.pdf).
- Schmid, Alex. 2013. The Definition of Terrorism. In *The Routledge Handbook of Terrorism Research*, ed. Alex Schmid, 38–98. Abingdon-on-Thames: Routledge.
- Schmid, Alex. 2014. *Violent and Non-Violent Extremism: Two Sides of the Same Coin?* The Hague: International Centre for Counter-Terrorism. <https://www.icct.nl/download/file/ICCT-Schmid-Violent-Non-Violent-Extremism-May-2014.pdf>.
- Scrivens, Ryan, Garth Davies, and Richard Frank. 2016. Searching for Signs of Extremism on the Web: An Introduction to Sentiment-Based Identification of Radical Authors. *Behavioural Sciences of Terrorism and Political Aggression* 10 (1): 39–59.
- Seib, Philip, and Dana M. Janbek. 2010. *Global Terrorism and New Media: The Post-Al Qaeda Generation*. Abingdon-on-Thames: Routledge.
- Selepak, Andrew. 2010. Skinhead Super Mario Brothers: An Examination of Racist and Violent Games on White Supremacist Web Sites. *Journal of Criminal Justice and Popular Culture* 17 (1): 1–47.
- Shane, Scott. 2016. The Enduring Influence of Anwar Al-Awlaki in the Age of the Islamic State. *Combating Terrorism Center Sentinel* 9 (7): 15–20.
- Sheikh, Jakob. 2016. “I Just Said It. The State”: Examining the Motivations for Danish Foreign Fighters in Syria. *Perspectives on Terrorism* 10 (6). <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/557>.
- Shortland, Neil D. 2016. “On the Internet, Nobody Knows You're a Dog”: The Online Risk Assessment of Violent Extremists. In *Violence and Society: Breakthroughs in Research and Practice*, 591–615. Hershey, PA: Information Science Reference.
- Silverman, Tanya, Christopher J. Stewart, Zahed Amanallah, and Jonathan Birdwell. 2016. *The Impact of Counter-Narratives: Insights from a Year-Long Cross-Platform Pilot Study of Counter-Narrative Curation, Targeting, Evaluation and Impact*. London: Institute for Strategic Dialogue. <https://www.Demos.co.uk/wp-content/uploads/2016/09/Counter-speech-on-facebook-report.pdf>.
- Simi, Pete, and Robert Futrell. 2006. Cyberculture and the Endurance of White Power Activism. *Journal of Political and Military Sociology* 34 (1): 115–42.
- Smith, Laura. 2017. In the Early 1980s, White Supremacist Groups Were Early Adopters (and Masters) of the Internet. *Timeline*, 11 October. <https://timeline.com/white-supremacist-early-internet-5e91676eb847>.
- Stalinsky, Steven, and R. Sosnow. 2017. Germany-Based Encrypted Messaging App Telegram Emerges as Jihadis' Preferred Communications Platform. MEMRI website, Lab Projects, 3 January. <https://www.memri.org/cjlab/germany-based-encrypted-messaging-app-telegram>

- emerges-as-jihadis-preferred-communications-platform-part-v-of-memri-series-encryption-technology-embraced-by-isis-al-qaeda-other-jihadis.
- Stenerson, Anne. 2013. "Bomb-Making for Beginners": Inside an Al-Qaeda E-Learning Course. *Perspectives on Terrorism* 7 (1): 25–37. <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/241/html>.
- Stevens, David, and Kieron O'Hara. 2015. *The Devil's Long Tail: Religious and Other Radicals in the Internet Marketplace*. London: Hurst.
- Stevens, Tim, and Peter Neumann. 2012. *Countering Online Radicalisation: A Strategy for Action*. London: International Centre for the Study of Radicalisation. <http://ic-sr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf>.
- Sullivan, Rachel. 2014. Live-Tweeting Terror: A Rhetorical Analysis of @Hsmprss\_ Twitter Updates during the 2013 Nairobi Hostage Crisis. *Critical Studies on Terrorism* 7 (3): 422–33.
- Taub, Ben. 2015. Journey to Jihad: Why are teenagers joining ISIS? *New Yorker*, May 25. <https://www.newyorker.com/magazine/2015/06/01/journey-to-jihad>.
- Torres-Soriano, Manuel Ricardo. 2012. The Dynamics of the Creation, Evolution, and Disappearance of Terrorist Internet Forums. *International Journal of Conflict and Violence* 7 (1): 1–14.
- Torres-Soriano, Manuel Ricardo. 2016. The Hidden Face of Jihadist Internet Forum Management: The Case of Ansar Al Mujahideen. *Terrorism and Political Violence* 28 (4): 735–49.
- Tuck, Henry, and Tanya Silverman. 2016. *The Counter-Narrative Handbook*. London: Institute for Strategic Dialogue. [http://www.isdglobal.org/wp-content/uploads/2016/06/Counter-narrative-Handbook\\_1.pdf](http://www.isdglobal.org/wp-content/uploads/2016/06/Counter-narrative-Handbook_1.pdf).
- United States Department of State. 2006. *Legislative Requirements and Key Terms*. Washington, DC. <https://www.state.gov/j/ct/rls/crt/2005/64331.htm>.
- Vermeulen, Floris, and Frank Bovenkerk. 2012. *Engaging with Violent Islamic Extremism*. The Hague: Eleven International.
- von Behr, Ines, Charlie Edwards, Luke Gribbon, and Anais Reding. 2013. *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Brussels: RAND Europe. [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR453/RAND\\_RR453.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf).
- Wagemakers, Joas. 2011. Al-Qa'ida's Editor: Abu Jandal Al-Azdi's Online Jihadi Activism. *Politics, Religion, and Ideology* 12 (4): 355–69.
- Weimann, Gabriel. 2004. *www.terror.net: How Modern Terrorism Uses the Internet*. Washington, DC: United States Institute of Peace.
- Weimann, Gabriel. 2006. Virtual Disputes: The Use of the Internet for Terrorist Debates. *Studies in Conflict and Terrorism* 29 (7): 623–39.
- Weimann, Gabriel. 2010. Terror on Facebook, Twitter, and Youtube. *Brown Journal of World Affairs* 16 (2): 45–54.
- Weimann, Gabriel. 2016. Terrorist Migration to the Dark Web. *Perspectives on Terrorism* 10 (3): 40–44. <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513>.
- Weimann, Gabriel, and Katharina von Knop. 2008. Applying the Notion of Noise to Countering Online Terrorism. *Studies in Conflict and Terrorism* 31 (10): 883–902.
- Weisburd, Aaron A. 2009. Comparison of Visual Motifs in Jihadi and Cholo Videos on YouTube. *Studies in Conflict and Terrorism* 32 (12): 1066–74.
- Wibtrope, Ronald. 2012. *Rational Extremism: The Political Economy of Radicalism*. Cambridge, UK: Cambridge University Press.
- Wiktorowicz, Quintan. 2003. *Islamic Activism: A Social Movement Theory Approach*. Bloomington: Indiana University Press.
- Wiktorowicz, Quintan. 2005. *Radical Islam Rising: Muslim Extremism in the West*. Oxford: Rowman and Littlefield.
- Winkler, Carol K. 2016. Visual Images: Distinguishing Daesh's Internal and External Communication Strategies. In *Countering Daesh Propaganda: Action-Oriented Research for Practical Policy Outcomes*, 15–20. Atlanta: Carter Center.
- Winkler, Carol K., Kareem El Damanhoury, Aaron Dicker, and Anthony F. Lemieux. 2016. The Medium is Terrorism: Transformation of the About to Die Trope in Dabiq. *Terrorism and Political Violence* 31 (2): 224–43. <http://www.tandfonline.com/doi/abs/10.1080/09546553.2016.1211526>.
- Winter, Charlie. 2015a. *The Virtual "Caliphate": Understanding the Islamic State's Propaganda Strategy*. N.p.: Quilliam. <https://www.stratcomcoe.org/charlie-winter-virtual-caliphate-understanding-islamicstates-propaganda-strategy>; accessed 10 January 2018.
- Winter, Charlie. 2015b. *Documenting the Virtual "Caliphate"*. Quilliam. <http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf>.
- Winter, Charlie. 2016. *An Integrated Approach to Islamic State Recruitment*. Barton, Australia: Australian Strategic Policy Institute. <https://www.aspi.org.au/report/integrated-approach-islamic-state-recruitment>.
- Zelin, Aaron Y. 2013. *The State of Global Jihad Online*. Washington, DC: New America Foundation. <http://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20130201-NewAmericaFoundation.pdf>.
- Zelin, Aaron Y. 2015. Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output. *Perspectives on Terrorism* 9 (4): 85–97. <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/445/html>.
- Zelizer, Barbie. 2010. *About to Die: How News Images Move the Public*. Oxford: Oxford University Press.