Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research

Maura Conway
maura.conway@dcu.ie

ABSTRACT
Some scholars and others are skeptical of a significant role for the Internet in processes of violent radicalization. There is increasing concern on the part of other scholars, and increasingly also policymakers and publics, that easy availability of violent extremist content online may have violent radicalizing effects. This article identifies a number of core questions regarding the interaction of violent extremism and terrorism and the Internet, particularly social media, that have yet to be adequately addressed and supplies a series of six follow-up suggestions, flowing from these questions, for progressing research in this area. These suggestions relate to (1) widening the range of types of violent online extremism being studied beyond violent jihadis; (2) engaging in more comparative research, not just across ideologies, but also groups, countries, languages, and social media platforms; (3) deepening our analyses to include interviewing and virtual ethnographic approaches; (4) up-scaling or improving our capacity to undertake "big data" collection and analysis; (5) outreaching beyond terrorism studies to become acquainted with, for example, the Internet Studies literature and engaging in interdisciplinary research with, for example, computer scientists; and (6) paying more attention to gender as a factor in violent online extremism.

The "slick" and "glossy" nature of the so-called Islamic State's (IS) online content and its resultant potential attractiveness to, and resonance with, discontented "digital natives" (i.e., young people who have grown up with the Internet) has been widely reported on in the world's press and is now a source of considerable public and governmental anxiety. There is no yet proven connection between consumption of and networking around violent extremist online content and adoption of extremist ideology and/or engagement in violent extremism and terrorism however.[1] Some scholars and others remain skeptical of a significant role for the Internet in processes of violent radicalization.[2] There is increasing concern on the part of other scholars, and increasingly also policymakers and publics, that high and increasing levels of always-on Internet access and the production and wide dissemination— and thence easy availability—of large amounts of violent extremist content online may have violent radicalizing effects,[3] which certainly appears to be one of the main purposes of its producers. Determining the significance of the role of the Internet in contemporary extremism and terrorism is not the goal of this article, however, and, indeed, is unlikely to be able to be adequately addressed in any single journal article given the scope of the issues necessary to be addressed. This article has a narrower remit: it contextualizes research and discussion in this area to date and proffers six suggestions for progressing research on the role of the Internet in violent extremism and terrorism so that we may be better placed to make a determination as to the significance of the Internet's role in the latter going forward. The article is composed of three sections. The first section provides context via summary of the nature of the research produced to date on the role of the Internet in violent extremism and terrorism.

Section two composes a brief re-cap of a variety of arguments for and against the Internet having a significant role in contemporary violent extremism and terrorism. Section three, the article's longest, identifies two core questions regarding the interaction of violent extremism and terrorism and the Internet, particularly social media, which have yet to be adequately addressed and supplies a series of six follow-up suggestions, flowing from these questions, for progressing research on violent online

extremism and terrorism. These suggestions are with respect to the necessity for researchers in this area to widen our research beyond violent online jihadism, engage in more comparative analysis, consider virtual ethnography as a viable approach while at the same time not dismissing upscaling techniques, draw from Internet studies and engage in interdisciplinary research, and consider gender as an important category. The conclusion reiterates that while ours is a burgeoning research field, it lacks a sound theoretical and evidential base.

Research to Date

A useful distinction may be drawn between descriptive research and explanatory research. Broadly, descriptive research asks "What is going on?" while explanatory approaches ask "Why is it going on?" Much descriptive research is scene-setting; it involves providing historical and/or contemporary overviews of some research topic or issue area by drawing together and synthesizing the available data. Abstract questions are not ruled out however. "Is the role of the Internet in contemporary terrorism increasing?" is a descriptive research question, for example. Explanatory research, on the other hand, largely develops causal explanations. Instead of asking whether the Internet has an increased role in contemporary terrorism, explanatory research might ask "Why is the Internet playing an increased role in contemporary terrorism?" It is one thing to show that the Internet is of greater significance in contemporary terrorism, in other words, but another thing altogether to explain why this is so. Research of both sorts is "fundamental to the research enterprise,"[4] unfortunately adequate amounts of neither have been undertaken on the role of the Internet in contemporary violent extremism and terrorism. It is impossible to adequately answer the question of why the Internet is playing a greater role in contemporary violent extremism and terrorism absent prior knowledge of what role, if any, the Internet is playing in the latter. Unfortunately, basic descriptive research is largely missing from this field, along with more complex theory-informed approaches seeking to show causal connections.[5] This is pretty astounding given the treasure trove of data now available online. It allowed William McCants, in testimony before the U.S. House of Representatives Homeland Security Subcommittee on Counterterrorism and Intelligence in December 2011, to raise the following in relation to what questions:

There is little research to go on, which is striking given how data-rich the Internet is. In hard numbers, how widely distributed was Zawahiri's last message? Did it resonate more in one U.S. city than another? Who were its main distributors on Facebook and YouTube? How are they connected with one another? This sort of baseline quantitative research barely exists at the moment.[6]

Aaron Zelin observed as recently as 2013 that:

More than 11 years after the attacks of 9/11 and nearly a decade since the rise of popular online jihadi Internet forums, there is strikingly little empirical research on the manner in which jihadi activists use the Web to propagate their cause. Whereas researchers and policy analysts have systematically collected and analyzed the primary source material produced by al-Qaeda and its allies, very little work has been done on the conduits through which that information is distributed— and even to what extent anyone is accessing that propaganda other than counterterrorism analysts.[7]

Missing, in other words, are analyses of individual Internet users' online activity and experiences in extremist cyberspaces, in addition to research on the online structures within which the latter are operating—even constrained—and the different workings and therefore functions of these. Neither what or why questions are being addressed, in other words.

Given these and other difficulties with the available research, it's unsurprising that there is ongoing debate among scholars about the significance of the Internet in contemporary violent extremism and terrorism, particularly its role in processes of violent radicalization.

Arguments for and Against a Significant Role for the Internet in Violent Extremism and Terrorism

Skepticism that the Internet might have a role to play in violent extremism and terrorism is not new. Walter Laqueur, an early and influential figure in Terrorism Studies, made the following observation in 1999: "No amount of email sent from the Baka Valley to Tel Aviv, from Kurdistan to Turkey, from the Jaffna peninsula to Colombo, or from India to Pakistan will have the slightest political effect. Nor can one envisage how in these conditions virtual power will translate into real power."[8] This is an interesting statement from a number of perspectives, chief among them being that just a few lines previously, on the very same page in fact, Laqueur says that audio-cassettes of Khomeini smuggled into Iran during his exile in Najaf and subsequently Paris significantly impacted the Iranian revolution.[9] So Laqueur readily admits the fact that audio-cassettes changed the course of Iranian history, but cannot see how Internet technologies could fundamentally change anything in relation to terrorism. His initial impetus, to assign a role to information and communication technologies in political violence movements, is in keeping with David Rapoport's wave theory of terrorism, an often overlooked aspect of which is the way technology, especially communications technology, can influence the types, timing, and spread of terrorism.[10] Laqueur's skeptical view nonetheless persists. Over a decade later, in 2011, Jason Burke, journalist and author of an excellent early book about Al Qaeda,[11] made the following observation about social media and its effects in terms of contemporary terrorism:

Twitter will never be a substitute for grassroots activism. In much of the Islamic world, social media is only for super-connected local elites or supporters in far-off countries. Neither are much use on the ground, where it counts. Social media can bring in donations or some foreign recruits. It can aid communication with some logistics and facilitate propaganda operations, but it is not much use in a firefight….Twitter won't help al-Shabaab retake Mogadishu or the Taliban reach Kabul in any meaningful way.[12]

Startlingly, Burke seems to think social media activity cannot be a substantive form of "grassroots activism," which he seems to imply must be "real world" activism. Second, he appears to think that not a great many people in the Arab and Muslim world(s) are social media users, which was untrue, even in 2011; five Arab countries (i.e., United Arab Emirates [UAE], Lebanon, Jordan, Kuwait, and Tunisia) had greater than 25 percent Facebook penetration at the end of 2011, for example.[13] Third, Burke says that Twitter is "not much use on the, ground, where it counts," while at the same time admitting that it can bring in donations, so it has a financing aspect; can attract so-called foreign fighters, so it has a recruitment function; and can also aid in communication, logistics, and propaganda. A single free online platform that can be employed for fund-raising, recruitment, information dissemination, and intra-group communications seems likely to be quite an important tool in arriving at, ultimately, the "firefight." This privileging of "real world" activity is shared by a diversity of commentators. Assertions that "most jihadists need to actually meet recruiters offline to be convinced to make the trip overseas"[14] or "Physical contact, in addition to online communication and propaganda, is essential"[15] are quite commonplace. An implicit privileging of the "real world" may also explain the contention contained in theU.K. House of Commons's Home Affairs Committee's counterterrorism report that:

The process of radicalisation will continue: the ideology which has come to be associated with al-Qa'ida will be more resilient than al-Qa'ida itself. Extremist material on the Internet will continue to motivate some people to engage in terrorism but will rarely be a substitute for the social process of radicalisation" [italics mine].[16]

Thence, in 2014, there were—likely still are—those in the U.K. government who think that the Internet is not social. They are either unaware of or have misunderstood the "social" aspects of "social media." Today's Internet does not simply allow for the dissemination and consumption of "extremist material" in a one-way broadcast from producer to consumer, but also high levels of online social interaction around this material. It is precisely the functionalities of the social Web that causes many scholars, policymakers, and others to believe that the Internet is playing a significant role in contemporary radicalization processes.

This is not to say that there are not more convincing arguments for the role of the Internet in contemporary violent radicalization having been oversold; these arguments take two main forms. One position holds that most, although not all, contemporary violent online extremists are dilettantes, in the sense that they restrict themselves to using the Internet to support and encourage violent extremism, but pose no "real world" threat. Put another way, there is the possibility that extremists' virtual "venting" or "purging" satisfies their desire to act. Their online activity, on this analysis, rather than becoming an avenue for violent radicalization and potentially ultimately "real world" action including, in the most extreme instances, terrorism, instead becomes for many a mechanism to dissipate the desire for violent action.[17] An associated argument is that many of those using the Internet to profess a dedication to or desire for violent action are engaged in a type of grandstanding common to the Internet, without ever having had any real commitment and/or intention to engage in violence at all. Even the United Kingdom's Government Communications Headquarters (GCHQ) has acceded that true intent can be very difficult to discern from online communications and activity.[18] The "online dis-inhibition effect," in its "toxic" form,[19] means that discussion of violent action and even direct threats of violence are so prevalent online that were all social media companies to share all postings of a violent extremist nature with authorities, the latter would be deluged with information and potentially rendered unable to function; the ultimately benign—or at least not directly resulting in "real world" violence—nature of most such vitriolic trolling is seen to make this unnecessary, however.

A second skeptical approach is to argue that claiming violent extremist online content violently radicalizes individuals is senseless given that other consumers of the same content are not similarly affected. In fact, large and growing numbers of researchers, journalists, and others are regularly exposed to substantial amounts of violent extremist content over long periods of time, but are not radicalized, never mind caused to engage in terrorism. On the contrary, the latter experience may even increase these consumers' abhorrence of violent extremism and terrorism, which may be supposed to be the opposite effect than intended by its producers.[20] There's no reason to expect that this is not the experience of large segments of the general public also. This is not the same thing, on the other hand, as saying consumption of violent extremist content has negligible effects on all those who consume it. MI5 asserts that *Inspire* magazine was "read by those involved in at last seven out of the ten attacks planned within the UK since its first issue [in 2010]."[21] The direction of causation remains unknown however: did reading *Inspire* cause the attack planners to plan the attacks? Did they begin attack planning and were then exposed to the magazine? Or did Inspire have different roles for different (groups of) attackers? Overall, the issue of the ratio of downloads/ views to attacks causes some to argue that while violent extremist content can buttress an already sympathetic individual's resolve to engage in violence, it is not generally the originating cause of such a commitment.[22] This may make intuitive sense, but is it borne out by the evidence?

It is estimated that Internet penetration in North America is c. 88 percent, in Europe is c. 70.5 percent, and in the Middle East is c. 48 percent.[23] Most scholars are inclined to agree, in this context, that along with all the other changes that it has wrought, the Internet is also affecting the conduct of contemporary violent extremism and terrorism. "Terrorism cases in the UK without a 'digital footprint' are increasingly rare," for example.[24] The former chief constable of West Yorkshire and U.K. Association of Chief of Police Officers (ACPO) head of Prevent, Norman Bettison, observed in 2012 that "the Internet features in most, but not all, terrorism cases."[25] This is a far cry, however, from Marc Sageman's assertion that "face-to-face radicalisation has been replaced by online radicalisation."[26] The vast majority of researchers grappling with the role of the Internet in contemporary violent extremism and terrorism—whether sceptics for a significant role, convinced of same, or located somewhere in between—now agree that the question is no longer if the Internet has a role to play in contemporary violent extremism and terrorism, but the more pertinent issue is determining its level of significance in contemporary violent radicalization processes. How do we know that most jihadis still need to meet recruiters offline to be convinced to travel overseas? This is no more likely, in the absence of sound data and analysis, than young women being "Brainwashed in their Bedrooms" via Twitter.[27] Both could be true, in fact; perhaps

gender is a determining factor. We just do not know enough at this stage as this whole research area is bereft of established empirical findings.

Where Do We Go From Here? Six Suggestions for Progressing Research

It is suggested that at least two foundational questions regarding the role of the Internet in violent extremism and terrorism are yet to be adequately addressed, never mind answered. These are:

1. Is it possible for persons to be radicalized online? In particular, can online interactions and/or consumption of violent and/or nonviolent online content cause some individuals to become violently radicalized?
2. If violent online radicalization[28] can be shown to occur, what are the contours of these processes? In particular, does the significance of the Internet in violent radicalization processes differ according to users' ideology, location, proximity to a given conflict, gender, types of online activity, preferred online platforms, and/or other factors?

There is little difficulty in finding appropriate cases or anecdotes to illustrate the array of arguments both for and against a decisive role for the Internet in contemporary radicalization processes. The reality however is that insufficient substantive empirically grounded social science research has been undertaken to date in order to allow us to convincingly answer these questions. The work that has been done is largely focused on analyzing digital content and not its producers or consumers (i.e., the audience), distribution mechanisms, or its functioning and effects.

Even if one accepts, in the absence of sound research—and many people do including, importantly, policymakers—but on the basis of common sense, anecdote, and the like that violent online radicalization is actually occurring, how can effective counter strategies be developed, if we do not know how it's occurring? This has not stopped a chorus of national leaders,[29] government ministers,[30] and intelligence chiefs[31] from calling on social media companies to do more to rid their platforms of violent extremist and terrorist content. This raises a host of potential difficulties, not least what exactly constitutes "terrorist content" and others around freedom of speech. Instead of wholesale removals of "terrorist content," it could be possible if better analysis was available to do quite targeted deletion of content shown to be directly implicated in violent radicalization and terrorism. Content control and/ or deletion measures are often advocated in conjunction with online CVE (countering violent extremism), in which more resources are promised to be invested by governments.[32] But how can we develop and deploy effective online CVE projects absent knowing who precisely these should be targeted at, what types of content are attractive to them, and what platforms are trafficked by these users? These are the kinds of answers that nobody appears to have at the present time.

How can we begin to remedy this? Below are six suggestions—there are surely a great many others; this is certainly not an exhaustive accounting, merely a first attempt—for progressing research and knowledge on the role of the Internet, especially social media, in violent extremism and terrorism.

Widen

Academics, media, policymakers, and others have a tendency to lose perspective when it comes to violent jihadi online activity, particularly that of IS. The amount of violent political extremist online content is increasing all the time and is not limited to purveyors of any one political ideology. Research on the role of the Internet in violent extremism and terrorism therefore needs to be widened beyond the present narrow focus on violent jihadi online content and interactions. In order to determine whether violent online radicalization is occurring, academic research needs to extend to inquire into the whole range of contemporary violent extremists and terrorists and their online activities. This includes so-called old terrorist organizations that still maintain online presences, all variants of the violent extreme right, and a range of others. This widening is necessary, if for no other reason, than to allow for

comparative research (of which more below); to ask how what the jihadis do is different from, but also how it may share similarities with, what other violent extremists are doing online and to come up with explanations for these, especially as pertaining to the alleged effectiveness of violent jihadis' online radicalization strategies.

The extreme right is particularly worth consideration as, along with a history of violence, it has a very long online history, dating to the earliest days of the public Internet in the mid-1980s.[33] The Stormfront online forum, which has proudly described itself as "the first White Nationalist site on the Web,"[34] has well over 11 million posts. As early as 1996, Stormfront's Don Black asserted that "Organizations have recruited through Stormfront, and through their Web pages that we've linked to"[35] while a report by the Southern Poverty Law Center (SPLC) alleges that in the period 2010–2014, almost 100 murders could be attributed to registered Stormfront users.[36] Stormfront recorded an average of some 5,800 threads per month between August 2012 and February 2015, which amounts to some 70,000 new threads per year.[37] By way of comparison, the top-tier jihadi forum al-Shumukh al-Islam, showed some 150 new threads per day in Spring 2012 for an average of circa 55,000 new threads per year.[38]

Stormfront's longevity, size, and notoriety means that it has attracted a certain amount of scholarly attention.[39] In fact, researchers' attention to the extreme right's online presences,[40] while not vast, dwarves the analysis conducted on the "new" media activity of "old" terrorist groups. According to the European Union's police agency, Europol, nationalist–separatist activity remains commonplace.[41] "Old" terrorist groups are still therefore very much in existence and maintain presences on "new" media, which have received very little attention from researchers in recent years. "The IRA [Irish Republican Army] is unquestionably the most heavily studied terrorist organisation of the past forty years"[42] and yet there are only a handful of analyses addressing (dissident) Irish Republican online activity, despite these being considered a real and ongoing threat and having a plethora of websites, forums, and social media accounts associated with them.[43] This dearth of attention extends to other "old" groups with very lengthy and active online presences including, for example, the Revolutionary Armed Forces of Colombia (FARC), the Kurdistan Workers' Party (PKK),[44] and even Hamas[45] and Hizbollah,[46] both of which have proved themselves profoundly mediasavvy and have highly resourced and extensive online presences.

Compare

Widening our present narrow focus on violent online jihadism to encompass a variety of other contemporary violent online extremisms will allow us to engage in much-needed cross-ideological analysis. This is the minimum necessary level of comparative research however; comparison within and across a number of other categories is also vital. These categories are: (1) groups, (2) countries, (3) languages, and (4) platforms.

Violent jihadism is an ideology to which a large number of widely dispersed groups subscribe. Today, most journalists, policy analysts, and researchers are focused on the online activity of just one group that subscribes to this ideology: IS; a host of other violent jihadi groups are active online, however, and thus also warrant attention. Research on the role of the Internet in the Syria and Iraq conflicts largely omits analysis of the online activity of violent Shi'a groups, which are definitely not absent from the Internet, for example.[47] Africa- based jihadi groups, including al-Shabab and Boko Haram, are also under-researched.[48] Boko Haram's online presence was, until quite recently, fairly low-level and amateurish, but this appears to be changing.[49] What influence will the latter's pledge of *Bay'ah* to IS have on the former's online activity and what, if any, will be the "real world" impact of these? Some types of violent extremism and terrorism are strongly linked with specific regions, countries, or locales varieties of nationalist-separatism or ethnic-separatism (e.g., Irish Republicanism, Ulster Loyalism)—whereas others are more diffuse in character (e.g., violent jihadism, neo-Nazism) having both national and transnational components and links. Consider the European Union: different Member States face different levels of threat from these different types of violent extremists and terrorists, with some states facing significant difficulties from just one or a small number of types of extremism and others routinely

dealing with violence perpetrated in the name of a wide variety of different extremisms. Germany, for example, has experienced violence on the part of violent jihadists, the extreme right, and the extreme left; Ireland, on the other hand, has a long history of terrorism associated with the Northern Ireland conflict, but has suffered no terrorism on the part of violent jihadists, the extreme right, or the extreme left. Interesting questions arise regarding the role of the Internet in more local extremisms versus those of a more transnational or even global character: Is the Internet more effective in one setting than the other? Do social media have different functions for extremists with a specific geographic affiliation versus those subscribing to more diffuse ideologies? How do the specific dynamics of local conflicts play out online?[50] The significance of the Internet in violent extremism and terrorism in specific locales has received scant scholarly attention to date, much less comparison across these.

Should an emphasis on geography be avoided when researching the Internet? The Internet is oftentimes portrayed as inherently global in character; rather than geography playing a determining role therefore, might language be a more important factor? In some cases, language and geography map onto each other, but in many instances they do not. Clearly many people beyond those in Arab countries are consumers of Arabic language jihadi online content; not enough research into this content and activity surrounding it has yet been produced and this needs to change.[51] Studying violent online political extremism within the European Union context without considering Arabic language content would be redundant therefore as would studying IS's online activity only in the context of its Arabic language content and not the host of content produced in or translated into other languages. The French language "jihadisphere," for example, is composed of contributors from France, Belgium, and other francophone countries, particularly those in North Africa.[52] The issue of translation is also relevant; questions that have not yet even been raised in this domain include: What types of extremist online content is produced by extremist and terrorist groups in multiple languages simultaneously and why? What type of extremist content is routinely translated by fans, into what languages, and why? This translation work might prove to be of particular import if an analysis of interactions within and between extreme right communities on Twitter that found that linguistic and geographical proximity were highly influential factors were to play out similarly in the jihadi "Twittersphere" and more widely.[53]

Finally, in terms of top-level comparison, a lot more comparative research needs to get underway within and across online platforms, particularly social media platforms. Violent extremists and terrorists are active on not just one online platform but, like the rest of us, increasingly operate across multiple platforms. The Pew Research Centre has found that multi-platform use was on the rise in 2014, with 52 percent of online American adults now using two or more social media sites, an increase of 10 percent from 2013.[54] Violent extremist and terrorist groups and individual extremists and fans may be expected, likewise, to maintain multiple official online presences, including dedicated websites, blogs, forums, and assorted social media accounts. Researchers need to be cognizant of this and to inquire into specific violent extremist groups/ideologies and how they operate across different social media platforms, websites, and forums, on the one hand, and also consider how a diversity of violent extremist groups/ideologies operate on specific platforms. Different social media platforms have different functionalities; how are these different functions exploited by violent extremists? What are the affordances of Twitter that make it so attractive to jihadis, for example, and how does their Twitter activity differ from, but also integrate with, their You- Tube activity? What, on the other hand, does the broad violent extremist landscape on Facebook look like? What does the violent extremist landscape of YouTube look like? And so on. It's worth noting here too that it's not just high profile social media platforms that are integral to violent extremist online networks, but a host of other file, text, and video upload sites[55] are also crucial nodes as are a diversity of other platforms such as, for example, lower profile social media,[56] Telegram, and the Internet Archive. Analyses of the latter are worthwhile not just in themselves, but also because "[t]he dominance of Twitter as the 'model organism' for social media big data analyses … skews analyses of mechanisms,"[57] particularly with respect to violent online jihadism.

Deepen

In addition to casting a wider ideological net and engaging in more comparative research, drilling downward is also necessary. A great deal of the research that has been done in this area to-date is focused on (mainly jihadi) online content, whether drawn from websites, forums, or social media. Von Behr et al. are therefore correct to underline that:

[T]here has been little attention to the individual internet users' experience online and usage of the internet in the process of radicalisation, that is, whether and how the internet is associated with a person coming to support terrorism or forms of extremism leading to terrorism. When academic accounts do analyse these individuals' engagement with the internet, they often do so by examining secondary sources or anecdotal evidence. The largely secondary and/or anecdotal basis of knowledge in this field points to a key gap in the academic research on radicalisation—namely access to and analysis of primary data on terrorist "users" of the internet.[58]

Von Behr and colleagues liaised with British police for the purposes of their study and this may be a route open to other U.K. researchers and those in other jurisdictions also. For those unable or unwilling to adopt this approach, collection of primary data will require some old-fashioned social science research, including interviewing, probably especially online interviewing[59] given that some of the currently ongoing conflicts that have significant terrorism and online components are not conducive to on-the-ground research.

Interviewing could allow us to gain a deeper and more contextualized understanding of who is behind varieties of violent extremist online content, what they believe their purposes are, and why they are so invested in this particular pursuit. We need to ask users producing and disseminating this content: What are the content's production processes (i.e., how is it produced)? Why it is they are producing and disseminating the content? Who are they targeting? Who do they believe they are influencing and to what end? And the consumers: How and where do they locate violent extremist content online? Why are they consuming it or what causes them to do so? What, precisely, is its attractiveness? How do they feel it has affected them? A particularly salient question would be whether a majority or minority of those encountered by interviewers are so-called prosumers, that is at the same time both producers and consumers of violent extremist online content. Given that the Internet is no longer a "new media," there are also increasing numbers of former extremists able to speak to the role (or not) of the Internet in their (de-)radicalization.[60]

At the group as opposed to the individual level, virtual, online, or digital ethnography is an under-utilized approach for digging deeper. "The objective of ethnography is to describe the lives of people other than ourselves, with an accuracy and sensitivity honed by detailed observation and prolonged first-hand experience."[61] Rather than individual lives, however, ethnographers are concerned with the systematic exploration of particular cultures, including particularly sub-cultures and countercultures. "Virtual ethnography" or "netnography" simply refers to the conduct of ethnographic research in online spaces.[62] Employing the latter in research into violent online extremist spaces is doubly attractive because not only would it allow researchers to develop embedded understandings of the "real" and "online" day-to-day lives of particular countercultural groups, but in fact is being undertaken by many of us albeit largely unknowingly already: "It took me a long time to even notice these things…but it didn't really register—it was background noise to me, stuff I needed to shove aside to get to the hard information about people and events."[63] Hegghammer is referring here to the way in which cultural products (i.e., music, poetry, etc.) and practices (i.e., clothing, beard styles, gestures) are largely overlooked by those studying extremism and terrorism because they are not immediately and obviously instrumental. Hegghammer's interest is in jihadi culture generally and so he laments that "It was not possible to do participant observation with groups this radical. Fortunately, though, the internet has made available a large amount of high-granularity primary sources that allow for a form of 'ethnography by proxy.'"[64]

For those of us whose primary interest is in violent extremist online cultures, however, the Internet is the "field" and online participant observation is a staple of our daily lives; we just need to make this work for us to a greater extent than presently. Why? Because the successfulness of IS's (online) strategy is probably at least partially predicated on a steady stream of attack footage, including beheading videos, but what if an additional important ingredient of its online "successfulness" is precisely the selfies, cat pictures, and food "porn" so prevalent across IS "fighters'" social media accounts? What virtual ethnographic approaches allow us to tap into is the soft power of the latter and thereby a potential explanation for why some violent extremists' online strategies are more effective than others. Certainly, for youthful online jihadi "fanboys" and "fangirls" Al Qaeda's online content was (and is) probably apprehended as remote, undirected, and boring, while IS's is familiar, interactive, and "cool," displaying as it does many of the signs of everyday youth online culture albeit with a violent jihadi twist. This is not to say, of course, that virtual ethnographic approaches are inclined to take online pronouncements and portrayals at face value; much of what happens online is, following Irving Goffman, "frontstage": "normative, conventional, and expected behavior meant for public viewing." A key advantage of deep and prolonged participant observation however, including in the online "field," is that it provides access to the "backstage" of groups' social lives: "Backstage behavior is meant to be hidden from the public eye, it occurs behind the scenes, and only intimates can participate in or witness it."[65] A clash of "frontstage" and "backstage" becomes fairly quickly apparent to observers of female involvement and portrayals in the violent jihadi online milieu, for example, of which more below.[66]

Upscale

At the same time that the above-suggested deepening is taking place, some large-scale data—I hesitate to use the term "big data"—collection and analysis also needs to be ongoing. There is a huge amount of "born digital" data now publicly available online; this data along with available tools for its analysis and visualization ought to be harnessed by violent online extremism researchers. Much of this data has a high level of ephemerality associated with it however and thus needs to be subject to continuous collection, formatting, and archiving, so that it may be readied for immediate quantitative and qualitative research and retained for future comparative analyses. Such analyses would provide, at a minimum, a big picture view of the contemporary violent online extremist scene and its various corners and allow us to identify areas in which to excavate further. What explains the lack of studies employing large datasets culled from violent extremist online spaces? I suggest it's because most researchers in this area are social scientists and thus do not have the necessary skills to easily collect, store, and analyze truly large quantities of online data. There are at least four ways to seek to hurdle this obstacle however: (1) work with computer scientists, (2) learn how to undertake basic online data collection and analysis ourselves, (3) build data archives and develop bespoke tools, (4) use commercial data brokers. Collaborating with colleagues from other disciplines, including computer science, is addressed in the next section, so let me briefly address points 2–4 here.

It's not impossible for social scientists to learn how to use basic online data collection and analysis tools, especially freely available open source software accompanied by clear "How To" documentation and online tutorials; Gephi data visualization software is one such accessible tool. This option is made more attractive when researchers have the opportunity to learn how to use these tools in dedicated "real world" tutorials and workshops, preferably tailored for social scientists.[67] Another option is to build, maintain, and make accessible archives of violent extremist online content for use by researchers. An example of this is the University of Arizona's Dark Web Forum Portal, which collected and makes available to researchers the content of 28 jihadi forums that together comprise nearly 13,000,000 messages.[68] This is an excellent resource, which has not been widely drawn on; one reason for this may be social scientists inability, as already mentioned, to handle not just collection, but also analysis of such "big data" (another reason may be the shift of focus from forums to social media in recent years). The relatively low level of Dark Web take-up could be altered, it is suggested, by making available easy-to-use analysis tools alongside data on a single platform, which is a planned outcome of the EU-funded

VOX-Pol project.[69] The final option is to employ the services of commercial social media data brokers, such as Gnip or DataSift,[70] which allow researchers to buy data from a multiplicity of social media platforms from a single supplier. Some downsides of this are the cost and the inability to freely share the data for replication and other purposes post-publication.

The difficulties of upscaling are not just of a practical sort, however. One of themost obvious difficulties is the issue of representativeness. Analyses drawing on large or even huge amounts of violent extremist content from the Internet and using it to explain violent online extremism have the propensity to be treated as "true" precisely because of the "hugeness" of the data and thereby its alleged representativeness. Selecting data on the basis of meeting a criteria and then using that data as evidence for the criteria (i.e., selecting on the dependent variable) is problematic, however. In the case of violent online extremism research, this is exacerbated by a recent further narrowing of focus to Twitter because of its particular affordances (e.g., ease of data collection due to its publicness) and thus introducing further sample selection bias. Layered atop all of this must be the further realization that "[s]ocial media data almost solely captures 'node-to-node' interactions, while 'field' effects—events that affect a society or a group in a wholesale fashion either through shared experience or through broadcast media—may often account for observed phenomena."[71] Put another way, there needs to be greater awareness among violent online extremism researchers that IS's Twitter activity, for example, while unlikely to be having no impact in terms of, say, attracting "foreign fighters," may be less impactful than IS's (and other violent jihadis) overall Internet-based campaign(s) that may, in turn, be much less impactful than other factors, such as IS's declaration of the caliphate, as an attraction factor. One of the only ways of determining this, to revert to an earlier point, would be to interview (former) "foreign fighters" and ask them about what influenced their decision making because "[s]ometimes, the only way to study people is to study people."[72]

Outreach

The original interest of most of those currently researching the intersection of violent extremism and terrorism and the Internet is violent extremism and/or terrorism rather than the Internet. This is easily remediable by, for example, exposing ourselves to new literatures beyond terrorism studies and/or direct outreach to colleagues in other disciplines. A literature that researchers in our field could usefully familiarize themselves with is Internet Studies while disciplines that we could perhaps most usefully collaborate with colleagues from include computational linguistics, computer science, information systems, and statistics. It is pertinent to ask about media and communication studies in general and Internet Studies, in particular what Richard Jackson asked about conflict analysis and peace research and its relationship to terrorism studies. "How is it," Jackson inquired:

that the "known" knowledge of the causes and resolution of violent political conflict (including conflicts where terrorism was present), which has accumulated from decades of conflict analysis and peace research, among others, remains largely "unknown" within the terrorism studies field? Why is it that within terrorism studies research continues apace on questions related to terrorism's causes and effective responses without reference to the key scholars and existing studies of peace and conflict studies?[73]

Reformulating Jackson's question then: "How is it that knowledge of the intersections of media and conflict (including conflicts where terrorism was present), which has accumulated from decades of media and communication research, among others, remains largely 'unknown' within the terrorism studies field? Why is it that within terrorism studies research there has been a surge of research on questions related to terrorism and the Internet, especially social media, without reference to the key scholars and existing studies of media and communication research generally and Internet studies particularly?" A ready answer to this question, which basically queries our lack of knowledge of other social scientists research, is much more difficult to supply than, say, a convincing answer to the question of why collaboration between social scientists and computer scientists or statisticians is not more prevalent.

Christina Archetti has contributed a book detailing the merits of a communication studies approach to *Understanding Terrorism in the Age of GlobalMedia*;[74] I want to emphasize here the necessity of drawing from Internet studies to enrich research on violent online extremism and terrorism. There is a large and increasing body of work done by Internet researchers that is germane to this particular sphere. Internet researchers have, for example, generated a significant amount of work on credibility and trust online, none of which deals directly with violent extremism or terrorism, but is nonetheless straightforwardly relevant in that it engages deeply with questions like how credibility is built online, how credibility is lost online, and so on.[75] Hegghammer's analysis of jihadi online forums is clearly enriched by his drawing from this literature;[76] few other terrorism researchers have followed his lead, however. Take another area of Internet research in which there are strongly consistent findings: the way in which discussion forums and other online spaces are generally dominated by a few "super contributors."[77] Berger and Morgan made a similar finding in their recent work on IS-related Twitter activity (i.e., of the network of 40,000 user accounts analyzed, c. 1,500–3,000 were prolific tweeters),[78] but omitted discussion of the way in which this is at least partially explainable by previous research on non-extremist online environments and thus is not unique to IS, albeit the latter have also been known to "game the system."[79] Having said this, *The ISIS Twitter Census* is an excellent example of a beneficial collaborative relationship between an extremism researcher and a technologist/data scientist, which does the important job of answering some of the what questions regarding IS's Twitter presence.

Truly interdisciplinary research is easier said than done; collaborating with colleagues from other disciplines, including computational linguistics and computer science, among others, is distinctly different than drawing from other social science fields like Communication Studies or Internet Studies. Research into the role of the Internet in violent extremism and terrorism is an area that would benefit hugely from the latter, however. It was suggested above that social scientists educate ourselves in the use of basic online data collection and analysis tools; for more sophisticated analyses, we need to work with those who not only have knowledge of the available tools and their deployment, but can tailor these further. This is not a one-way relationship with computer scientists benefiting their social science colleagues in the absence of benefit to themselves; the best outcomes are obtained by computer scientists collaborating with domain experts, in this case those with knowledge of the ideologies prevalent within and day-to-day workings of online extremism. Increased collaboration between social scientists, especially terrorism studies scholars, and computer scientists is the most pressing, but there are a host of other colleagues we could doubtless also benefit from collaborating with (e.g., law, criminology, psychology).

Gender

The preceding five sub-sections dealt largely with broad brush methodological or "how to" issues, this sub-section is somewhat different. In it I want to emphasize both how some of my earlier points apply, but also how the study of gender is particularly pertinent in violent online extremism.

Al-Khansa, the first online jihadi magazine targeted specifically at women, appeared in 2004. Stormfront's "Ladies Only" sub-forum was established in 2007 and has 1,156 threads and 48,789 posts at time of writing. Astoundingly, given their relative visibility and after more than a decade of research, the online activity of jihadi and extreme right females is the subject of less than a handful of studies.[80] Women featured fairly prominently on the websites of the FARC, New People's Army, and Tamil Tigers in the 1990s and early 2000s; the role of ethnic-nationalist or nationalist-separatists women online has been the subject of no research at all however. The role and influence of women in violent extremist cyberspaces is therefore largely unknown. A number have clearly played powerful roles online that may not have been afforded them in more conventional settings including, for example, Malika El-Aroud's central role in the establishment of the French-language "jihadisphere."[81] When addressed, it is generally female extremists' power as online motivators of their male counterparts that is highlighted[82]

albeit the role of so-called jihadi brides resident in Syria in persuading other young women to follow in their footsteps has received considerable recent global media attention. In terms of widening therefore, an additional step omitted earlier is to include women as a category of violent online extremists. Study of the gender dimensions of violent extremist and terrorist online activity does not, indeed *should* not, be restricted to female users, however. Not all, probably not even most, portrayals of women and their roles in violent extremism and terrorism are by women, but are instead depictions of women's roles as assigned by men. Interesting comparison would be between the depiction of jihadi women and their roles in official online publications, such as *al-Khansa*, *Inspire*, and *Dabiq*, versus the desired roles expressed by women in their social media activity and in other online spaces or the portrayal of women in violent jihadi cyberspaces versus in extreme right cyberspaces. How has the portrayal of women changed over time? If we ascertain an increased role for and influence of women in extremist cyberspaces in the last decade, can we link this to changes in the volume and types of depictions of women over the same period or are there other factors at play?

A number of images of violent jihadi women "training" with guns and posing with weapons around a luxury car have become well-known via social media and their reproduction in the Western press. It is suggested that these images go to distinctions between "frontstage" and "backstage" portrayals of the role of women in violent jihadism alluded to earlier, because they are carefully constructed "frontstage" portrayals of "romance" and adventure almost wholly outside of "normal" female jihadi activity in Syria. The vast majority of violent jihadi videos and other online content are striking, in fact, for their almost complete absence of female bodies. An Arabic language text that was circulated widely in Arab jihadi online networks, but not available in English until translated by a U.K. researcher, is probably more indicative of the "jihadi bride" experience than the "girls with guns" images. The Arabic document entitled "Women in the Islamic State" is unequivocal regarding female roles: "the greatness of her position, the purpose of her existence is the Divine duty of motherhood." It goes on to extol the virtues of being a dutiful wife—a role that may appropriately be fulfilled from the age of nine—and the necessity of women remaining within the walls of their homes at almost all times.[83] The document is an interesting item of content in itself, but is also a noteworthy instance both of how online audiences may continue to be separated quite effectively by language and, relatedly, an awareness on the part of IS of the desire of some young women to play a more central role than that of simply *muhajirat* or "migrants" and thus IS's attempts at constructing a more attractive online narrative for these. The competing online constructions are drawn together in a tweet by one young woman: "I wonder if I can pull a Mulan and enter the battle field."[84]

"Pulling a Mulan" refers to the Disney film in which a young woman impersonates a man to join the military. While the likelihood of successfully carrying off such an impersonation in "real life" is improbable, gender-switching is commonplace online. From its earliest days the Internet was viewed by some as the ideal realm in which to "play" with their gender. Online gender-switching has been extensively studied in online gaming.[85] What is the likelihood of high levels of gender-switching in, say, jihadi online spaces? Early research on radicalization via YouTube found that that the higher one's status within the online group studied, on several different measures, the less likely one was to provide information about one's gender. Of the top ten users who frequently ranked in the top three of various social network measures in the study, five were of unknown gender and five identified themselves as female. It was thus surmised that at least some of the five users of unknown gender were probably in fact female.[86] This is not without precedent; in the past jihadi online forums were often segregated on the basis of gender. Anecdotal evidence collected by the author suggests that female researchers accessing extremist forums of various sorts are wont to adopt male personae, including screen names and avatar images, in those settings, but that male researchers retain male identities in the same circumstances. This is a potentially interesting phenomenon facilitated by the Internet that could mean that female users are more influential in extremist cyberspaces than previously thought. (Switching in the other direction is a possibility too, of course, and also has the potential for interesting findings [87]).

Conclusion

In closing, and by way of full disclosure, I am somebody who believes the Internet is playing significant and diverse roles in contemporary violent extremism and terrorism. Rapoport argues that structural factors are very important in terms of influencing the various waves of terrorism identified by him. Historically, new communication technologies (e.g., mass circulation newspapers, radio, audio cassettes, TV) have been shown to be particularly influential and have a history of transforming terrorism; the Internet is unlikely to be any different. Given the resources, in terms of both time and money, they are inputting to online campaigns, a diversity of contemporary violent extremists certainly thinks it's having an impact too. Some of the anecdotal evidence is also compelling. Taking just IS: online outreach to young women has resulted in an influx of "jihadi brides" to Syria, similar online calls for families to migrate to the "caliphate" have seen an uptick in family groups departing various countries, and a spate of previously uncommon types of terrorist attacks (e.g., running down people with cars, knifings) appear to correlate with online calls for these types of attacks to be undertaken. None of this is sufficient of course; what needs to be supplied is theoretically sound, empirically verifiable, social science research detailing—I hesitate to use the word "proving" in a social science context, especially this social science context—the role of the Internet in contemporary radicalization processes.

The earliest piece of analysis on violent extremism and the Internet appeared in 1985,[88] but the vast bulk only began to be produced in the 2000s, with a significant uptick since c.2010 and a particular spike in the past twelve months. Research in this area is thus not long underway and so, of course, there are many what and why questions still to be asked and answered. The nature of the Internet means that it changes very fast; it is thus quite difficult to effectively research the Internet and its workings over time. Direct audience research is also problematic because of the nature of violent extremist and terrorist online content, which presents problems for undertaking the kinds of experiments that are standard in other areas of Internet audience research as it would require introducing subjects to online content with allegedly radicalizing effects and, in fact, almost certainly necessitate exposing youth and young adults to distressing levels of violence. Progressing research in this area is thus not easy; it is not impossible either however. There are, of course, a whole host of issues that it was not possible to address in this article (e.g., Internet research ethics, the role of Internet companies as political intermediaries), but what it seeks to do is to make six major practical suggestions for progressing research on the role of the Internet in contemporary violent extremism and terrorism with, perhaps, the side-effect of also kick-starting discussion of colleagues' additional or preferred steps in this regard.

Funding

Notes

1. William McCants, "Testimony, U.S. House of Representatives, Subcommittee on Counterterrorism and Intelligence, Jihadist Use of Social Media: How to Prevent Terrorism and Preserve Innovation," 6 December 2011. Available at http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20McCants.pdf (accessed 27 March 2015); Diana Rieger, Lena Frischlich, and Gary Bente, *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos* (Cologne, Germany: Wolters Kluwer, 2013).
2. David C. Benson, "Why the Internet is Not Increasing Terrorism," *Security Studies* 23(2) (2014), pp. 293–328; Noemie Bouhana and Per-Olof H. Wikstrom, *Al-Qa'ida-influenced Radicalisation: A Rapid Evidence Assessment Guided by Situational Action Theory* (London: UK Home Office, 2011); Jonathan Githens-Mazer, "Radicalisation Via YouTube? It's Not So Simple," *The Guardian*, 4 November 2010. It's worth mentioning here too the contestability of "radicalization" as a concept as discussed in, for example, Akil Awan, Andrew Hoskins, and Ben O'Loughlin, *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (London: Routledge, 2012).
3. J. M. Berger and Bill Strathearn, *Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Extremism in Online Social Networks* (King's College London: ICSR, 2013); Joseph Carter, Shiraz Maher, and

Peter Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks* (King's College London: ICSR, 2014); Charlie Edwards and Luke Gribbon, "Pathways to Violent Extremism in the Digital Era," *RUSI Journal* No. 158 (2013), pp. 40–47; David H. Gray and Albon Head, "The Importance of the Internet to the Post-modern Terrorist and its Role as a Form of Safe Haven," *European Journal of Scientific Research* 25(3) (2009); Anne Stenersen, "The Internet: A Virtual Training Camp?," *Terrorism and Political Violence* 20(2) (2008); United Nations Independent International Commission of Inquiry on the Syrian Arab Republic, *Rule of Terror: Living under ISIS in Syria* (New York: UN, 2014), p. 4.

4. David De Vaus, *Research Design in Social Research* (London: Sage, 2001), p. 1.

5. Cristina Archetti, *Understanding Terrorism in the Age of Global Media: A Communication Approach* (Basingstoke: Palgrave, 2013), pp. 21–22.

6. McCants, "Testimony."

7. Aaron Zelin, *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis* (Washington, DC: New America Foundation, 2013), p. 1. See also, on conduits, Daniel Kimmage, *The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message* (Washington, DC: Radio Free Europe/Radio Liberty, 2008); Daniel Kimmage and Kathleen Ridolfo, *Iraqi Insurgent Media: The War of Images and Ideas* (Washington, DC: Radio Free Europe/Radio Liberty, 2007).

8. Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), p. 262.

9. As borne out in, for example, Annabelle Sreberny and Ali Mohammadi, *Small Media, Big Revolution: Communication, Culture, and the Iranian Revolution* (Minneapolis: University of Minnesota Press, 1994).

10. David Rapoport, "The Four Waves of Rebel Terror and September 11," *Anthropoetics* 8(1) (2002). Available at http://www.anthropoetics.ucla.edu/ap0801/terror.htm?gobackD.gde_3131037_member_5798090843084578819 (accessed 27 March 2015).

11. Jason Burke, *Al-Qaeda: Casting a Shadow of Terror* (London and New York: I.B. Tauris, 2003).

12. Jason Burke, "Al-Shabab's Tweets Won't Boost its Cause," *The Guardian*, 16 December 2011.

13. Arab Social Media Report, "Dynamic Dashboard: Facebook Penetration, 31 December 2011." Available at http://www.arabsocialmediareport.com/Facebook/LineChart.aspx?&PriMenuIDD18&CatIDD24&mnuDCat (accessed 27 March 2015).

14. Jamie Bartlett, "You Can't Prevent Terrorism by Singling Out Muslims," *The Telegraph*, 19 February 2015.

15. Hanna Rogan, *Jihadism Online: A Study of How al-Qaida and Radical Islamist Groups Use the Internet for Terrorist Purposes* (Norway: FFI, 2006), p. 30.

16. House of Commons Home Affairs Committee, *Counter-Terrorism: Seventeenth Report of Session 2013–14* (London: The Stationery Office, 2014), pp. 6–7.

17. Awan et al., *Radicalisation and Media*, pp. 58–59 and 64–65; Gilbert Ramsay, "Relocating the Virtual War," *Defence Against Terrorism Review* 2(1) (2009), p. 35.

18. Intelligence and Security Committee of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* (UK: Her Majesty's Stationery Office, 2014), p. 131.

19. John Suler, "The Online Disinhibition Effect," *International Journal of Applied Psychoanalytic Studies* 2(2) (2005). See also Jamie Bartlett, *The Dark Net* (London: Windmill Books, 2015), pp. 41–42.

20. Cristina Archetti, "Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age," *Perspectives on Terrorism* 9(1) (2015), p. 50.

21. As quoted in Intelligence and Security Committee of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*, p. 60; see also Alexander Meleagrou-Hitchens, *As American as Apple Pie: How Anwar al Awlaki Became the Face of Western Jihad* (King's College London: ICSR, 2011), p. 56.

22. Jonathan Githens-Mazer, "Radicalisation Via YouTube?"; Ghaffar Hussain and Erin Marie Saltman, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It* (London: Quilliam Foundation, 2014); Marc Sageman, *Understanding Terror Networks* (Philadelphia: Pennsylvania University Press, 2004), 163; Tim Stevens and Peter Neumann, *Countering Online Radicalisation: A Strategy for Action* (King's College London: ICSR, 2009), ch. 2.

23. "Internet World Stats." Available at http://www.internetworldstats.com/stats.htm (accessed 27 March 2015).

24. Ines von Behr et al., *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (Brussels and Cambridge: Rand Europe, 2013), p. 3.

25. As quoted in ibid., p. 5.

26. Marc Sageman, "The Next Generation of Terror," *Foreign Policy* (March/April 2008), p. 41. Sageman argued in previous work that the Internet was an important facilitator, but unlikely to transcend the necessity for face-to-face connections for development of deep interpersonal ties: *Understanding Terror Networks*, pp. 157 and 163.

27. Chris Greenwood et al., "Brainwashed in their Bedrooms: British Schoolgirl 'Jihadi Brides who Fled to Syria to Join ISIS' were Following SEVENTY Extremists on Twitter Accounts that the Internet Giant had Refused to Axe," *Daily Mail*, 22 February 2015.

28. Violent online radicalization is conceived herein as "a process whereby individuals, through their online interactions and exposure to various types of Internet content, come to view violence as a legitimate method of solving social and political conflicts" per Adam Bermingham et al., "Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation," in *ASONAM 2009: Advances in Social Networks Analysis and Mining* (IEEE Computer Society: Digital Library, 2009), p. 1.

29. See, for example, Kevin Rawlinson, "Sanction Tech Firms Over Hate Speech' says Hollande," *BBC News*, 28 January 2015; Nicolas Watt and Patrick Wintour, "Facebook and Twitter have 'Social Responsibility' to Help Fight Terrorism, says David Cameron," *The Guardian*, 16 January 2015.

30. See, for example, the Joint Statement of EU Ministers of the Interior and/or Justice condemning the Charlie Hebdo attacks, Paris, 11 January 2015. Available at https://eu2015.lv/images/news/2015_01_11_Joint_statement_of_ministers_for_interrior.pdf (accessed 27 March 2015).

31. See, for example, Robert Hannigan (the director of the UK's Government Communications Headquarters, GCHQ), "The Web is a Terrorist's Command-and-Control Network of Choice," *Financial Times*, 3 November 2014; remarks by U.S. Central Intelligence Agency Director John O. Brennan at the Council on Foreign Relations, Washington DC, 13 March 2015. Available at https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/directorbrennan-speaks-at-the-council-on-foreign-relations.html (accessed 27 March 2015).

32. The Australian government announced the Combating Terrorist Propaganda in Australia initiative at the February 2015 White House Summit on Countering Violent Extremism, which commits AUS$17.9 million "to combat the lies and propaganda terrorist groups are promulgating online." Media release available at http://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/20-February-2015-Combating-terrorist-propaganda-online.aspx (accessed 27 March 2015).

33. Anti-Defamation League (ADL), *Computerized Networks of Hate: An ADL Fact Finding Report* (New York: ADL, 1985). Available at https://archive.org/details/ComputerizedNetworksOfHate (accessed 27 March 2015).

34. Jennifer Oldham, "Web of Hate is Growing on the Net," *The Jerusalem Post*, 25 January 1998.

35. Reid Kanaley, "Hate Groups Tap into the Internet," *The Philadelphia Inquirer*, 4 July 1996.

36. Heidi Beirich, "White Homicide Worldwide," *SPLC Intelligence Report*, Summer 2014. Available at http://www.splcenter.org/sites/default/files/downloads/publication/white-homicide-worldwide. pdf (accessed 27 March 2015), pp. 2–6.

37. Unpublished research by the author recorded 680,000 threads on Stormfront in August 2012; at time of writing, in February 2015, Stormfront was showing 861,972 threads. The figure for average new threads monthly reported here were arrived at by calculating the number of threads initiated between August 2012 and February 2015 (i.e., 181,972) and dividing this by the number of months elapsed (i.e., 31).

38. Aaron Zelin, *The State of Global Jihad Online*, p. 8; see also Thomas Hegghammer, "Interpersonal Trust on Jihadi Internet Forums," in Diego Gambetta, ed., *Fight, Flight, Mimic: Identity Signaling in Armed Conflicts* (forthcoming). Available at http://hegghammer.com/_files/Interpersonal_trust.pdf (accessed 27 March 2015), p. 5.

39. See, for example, Lorraine Bowman-Grieve, "Exploring Stormfront: A Virtual Community of the Radical Right," *Studies in Conflict & Terrorism* 32(11) (2009); Willem De Kostera and Dick Houtman, "Stormfront is like a Second Home to Me: On Virtual Community Formation by Right-Wing Extremists," *Information, Communication, and Society* 11(8) (2008); Priscilla M. Meddaugh and Jack Kay, "Hate Speech or 'Reasonable Racism'? The Other in Stormfront," *Journal of Mass Media Ethics* 24(4) (2009).

40. See, for example, Josh Adams Vincent J. Roscigno, "White Supremacists, Oppositional Culture and the World Wide Web," *Social Forces* 84(2) (2005), pp. 759–778; Denise M. Bostdorff, "The Internet Rhetoric of the Ku Klux Klan: A Case Study in Web Site Community Building Run Amok," *Communication Studies* 55(2) (2004); Val Burris, Emery Smith, and Ann Strahm, "White Supremacist Networks on the Internet," *Sociological Focus* 33(2) (2000); Manuela Caiani and Linda Parenti, *European and American Extreme Right Groups and the Internet* (London: Ashgate, 2013); Manuela Caiani and Claudius Wagemann, "Online Networks of the Italian and German Extreme Right," *Information, Communication & Society* 12(1) (2009); Bart Cammaerts, "Radical Pluralism and Free Speech in Online Public Spaces: The Case of North Belgian Extreme Right Discourses," *International Journal of Cultural Studies* 12(6) (2009); Michael Chau and Jennifer Xu, "Mining Communities and Their Relationships in Blogs: A Study of Online Hate Groups," *International Journal of Human-Computer Studies* 65(1) (2007); Peter Chroust, "Neo-Nazis and Taliban On-line: Anti-modern Political Movements and Modern Media," *Democratization* 7(1) (2000), pp. 102–118; Phyllis Gerstenfeld, Diana Grant, and Chau-Pu Chiang, "Hate Online: A Content Analysis of Extremist Internet Sites," *Analyses of Social Issues and Public Policy* 3(1) (2003); Luca Tateo, "The Italian Extreme Right On-line Network: An Exploratory Study Using an Integrated Social Network Analysis and Content Analysis Approach," *Journal of*

Computer-Mediated Communication, 10(2) (2005); Georgie Weatherby and Brian Scoggins, "A Content Analysis of Persuasion Techniques Used on White Supremacist Websites," *Journal of Hate Studies* 4(9) (2005/6).

41. Europol, *TE-Sat 2015: European Union Terrorism Situation and Trend Report 2015* (The Hague: Europol, 2015); Europol, *TE-Sat 2014: European Union Terrorism Situation and Trend Report 2014* (The Hague: Europol, 2014).

42. Andrew Silke, "The Impact of 9/11 on Research on Terrorism," in Magnus Ranstorp, ed., *Mapping Terrorism Research: State of the Art, Gaps and Future Direction* (London: Routledge, 2007), p. 84.

43. Lorraine Bowman-Grieve, "Irish Republicanism and the Internet: Support for New Wave Dissidents," *Perspectives on Terrorism* 4(2) (2010), pp. 22–34; Lorraine Bowman-Grieve and Maura Conway, "Exploring the Form and Function of Dissident Irish Republican Online Discourses," *Media, War & Conflict* 5(1) (2012), pp. 71–85; Michael Dartnell, "The Electronic Starry Plough: The E-nationalism of the Irish Republican Socialist Movement (IRSM)," *First Monday* 6(12) (2001); Ross Frenett and M. L. R. Smith, "IRA 2.0: Continuing the Long War—Analyzing the Factors Behind Anti-GFA Violence," *Terrorism and Political Violence* 24(3) (2012), pp. 375–395; John Nalton, Gilbert Ramsey and Max Taylor, "Radicalization and Internet Propaganda by Dissident Republican Groups in Northern Ireland Since 2008," in P. M. Currie and Max Taylor, eds., *Dissident Irish Republicanism* (New York: Continuum, 2011), pp. 119–14; Paul Reilly, *Framing the Troubles Online: Northern Irish Groups and Website Strategy* (Manchester: Manchester University Press, 2011).

44. The FARC's lengthy online presence does not appear to have a single article or chapter dedicated to it, while the PKK's online presence appears to be the subject of just two chapters: Erdogan Celebi, "Analysis of PKK/KONGRA-GEL Websites to Identify Points of Vulnerability," in NATO Centre of Excellence for Defence Against Terrorism, eds., *Responses to Cyberterrorism* (Amsterdam: IOS Press, 2008); Erdogan Celebi, "Female Separatism: The Role of Women in the PKK/Kongra-Gel Terrorist Organization," in Hans-Liudger Dienel, Y. Sharan, Christian Rapp, and Niv Ahituv, eds., *Terrorism and the Internet: Threats, Target Groups, Deradicalisation Strategies* (Amsterdam: IOS Press, 2010). I analyze the FARC and PKK websites, along with others, in Maura Conway, "Terrorist Web Sites: Their Contents, Functioning, and Effectiveness," in Philip Seib, ed., *Media and Conflict in the Twenty-First Century* (New York: Palgrave, 2005).

45. In-depth studies of Hamas's online activity—as opposed to mention of their websites in analytical overviews of a diversity of violent extremist groups' virtual activity—are also astoundingly few: Tomer Mozes and Gabriel Weimann, "The E-Marketing Strategy of Hamas," *Studies in Conflict and Terrorism* 33(3) (2010). See also Conway, "Terrorist Websites."

46. Again, given Hizbollah's acknowledged media-savvy, analyses of their Internet acumen are scant: Maura Conway, "Terrorism and the Making of the 'New Middle East': New Media Strategies of Hizbollah and al Qaeda," in Philip Seib, ed., *New Media in the New Middle East* (London: Palgrave, 2007); Maura Conway, "Cybercortical Warfare: Hizbollah's Internet Strategy," in Sarah Oates, Diana Owen, and Rachel Gibson, eds., *The Internet and Politics: Citizens, Voters and Activists* (London: Routledge, 2005); Rune Friberg Lyme, *Hizb'allah's Communication Strategy: Making Friends and Intimidating Enemies* (Copenhagen: Danish Institute for International Studies, 2009). See also Conway, "Terrorist Web Sites."

47. The only scholarly analysis that I am aware of that treats this issue in any depth is Philip Smyth's "The Shiite Jihad in Syria and It's Regional Effects," *Policy Focus* No. 138. Available at https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus138_Smyth-2.pdf (accessed 26 April 2015). It's worth noting here too that Syrian government forces, Free Syrian Army units, the PKK and Kurdish Peshmerga forces, and other parties to the Syria conflict also maintain online presences and engage via the Internet, another issue that has not received sufficient scholarly attention to date.

48. Stewart Bertram and Keith Ellison, "Sub-Saharan African Terrorist Groups' Use of the Internet," *Journal of Terrorism Research* 5(1) (2014); Fredrick Romanus Ishengoma, "Online Social Networks and Terrorism 2.0 in Developing Countries," *International Journal of Computer Science & Network Solutions* 1(4) (2013); Alexander Meleagrou-Hitchens, Shiraz Maher, and James Sheehan, *Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy* (King's College London: ICSR, 2012); Lindsay Pearlman, "Tweeting to Win: Al-Shabaab's Strategic Use of Microblogging," *Yale Review of International Studies* Nov. 2012. Available at http://yris.yira.org/essays/837 (accessed 27 March 2015); Rachel Sullivan, "Live-Tweeting Terror: A Rhetorical Analysis of @HSMPress_ Twitter Updates During the 2013 Nairobi Hostage Crisis," *Critical Studies on Terrorism* 7(3) (2014).

49. "Is Islamic State Shaping Boko Haram Media?" *BBC Monitoring*, 4 March 2015 http://www.bbc.com/news/world-africa-31522469 (accessed 27 March 2015).

50. Aurelie Campana and Benjamin Ducol, "Voices of the 'Caucasus Emirate': Mapping and Analyzing North Caucasus Insurgency Websites," *Terrorism and Political Violence* 27(4) (2015), pp. 679–700.

51. An exception is Charlie Winter, *Documenting the Virtual Caliphate* (London: Quilliam Foundation, 2015).

52. Benjamin Ducol, "Uncovering the French-speaking Jihadisphere: An Exploratory Analysis," *Media, War & Conflict* 5(1) (2012).

53. Derek O'Callaghan et al., "An Analysis of Interactions Within and Between Extreme Right Communities in Social Media," *Lecture Notes in Computer Science* 8329 (2013).

54. Maeve Duggan et al, "Social Media Update 2014," Pew Research Centre: Internet Science and Tech Report, 9 January 2015. Available at http://www.pewinternet.org/2015/01/09/social-mediaupdate- 2014/ (accessed 27 March 2015).

55. Justpaste.it is a particularly important node in the contemporary violent jihadi online scene; Pastebin and Paste.ee are also used as repositories. In terms of video-hosting, Dailymotion, Media- Fire, Vid.me, Vimeo, and a host of other more obscure sites (e.g., Hugefiles.net, Uploadhero.com, Uptobox.com) are also employed.

56. These include Ask.fm, Diaspora, Flickr, Instagram, SoundCloud, Tumblr, VKontakte, and others.

57. Zeynep Tufekci, "Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls." Available at http://arxiv.org/ftp/arxiv/papers/1403/1403.7400.pdf (accessed 30 November 2015), p. 2.

58. von Behr et al., *Radicalisation in the Digital Era*, p. 8.

59. Janet E. Salmons, *Qualitative Online Interviews: Strategies, Design, and Skills* (London: Sage, 2014).

60. Daniel Kohler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization* 1 (Winter 2014/15).

61. Tim Ingold, "Anthropology is Not Ethnography," *Proceedings of the British Academy* 154 (2008), p. 69.

62. Christine Hine, Virtual Ethnography (London: Sage, 2000); Robert Kozinets, *Netnography: Doing Ethnographic Research Online* (London: Sage, 2009).

63. Thomas Hegghammer, "Why Terrorists Weep: The Socio-Cultural Practices of Jihadi Militants" (Paul Wilkinson Memorial Lecture, University of St. Andrews, April 16, 2015), p. 2. Available at http://hegghammer.com/_files/Hegghammer_-_Wilkinson_Memorial_Lecture.pdf (accessed 21 April 2015).

64. Ibid., p. 8.

65. Victor C. De Munck, "Participant Observation: A Thick Explanation of Conflict in a Sri Lankan Village," in Victor C. de Munck and Elisa J. Sobo, eds., *Using Methods in the Field: A Practical Introduction and Casebook* (Oxford: Oxford University Press, 1998), p. 43.

66. Erika Pearson, "All The World Wide Web's a Stage: The Performance of Identity in Online Social Networks," *First Monday* 14(3) (2009).

67. See, for example, the University of Amsterdam's Digital Methods Initiative at https://www.digitalmethods.net (accessed 21 April 2015), particularly their Summer and Winter Schools.

68. See http://ai.arizona.edu/research/terror (accessed 21 April 2015).

69. For more information, see http://www.voxpol.eu (accessed 21 April 2015).

70. See https://gnip.com and http://datasift.com (accessed 21 April 2015). Datasift supplied access to the Twitter "firehose" up until mid-April 2015, when this was retracted by Twitter from all partners excepting Gnip, which Twitter now owns.

71. Tufekci, "Big Questions for Social Media Big Data," p. 1.

72. Ibid., p. 6.

73. Richard Jackson, "Unknown Knowns: The Subjugated Knowledge of Terrorism Studies," *Critical Studies on Terrorism* 5(1) (2012), p. 12.

74. Archetti, *Understanding Terrorism in the Age of Global Media*.

75. See, for example, Gordon Bowen and Richard Bowen, "Brand Trust in Offline and Online Environments: Lessons for Social Media," in Gordon Bowen and Wilson Ozue, eds., *Computer-Mediated Marketing Strategies: Social Media and Online Brand Communities* (Hershey, PA: IGI Global, 2015); Jo Bryce and James Fraser, "The Role of Disclosure of Personal Information in the Evaluation of Risk and Trust in Young Peoples' Online Interactions," *Computers in Human Behavior* 30 (2014); Charles E. Naquin, and Gaylen D. Paulson, "Online Bargaining and Interpersonal Trust," *Journal of Applied Psychology* 88(1) (2003); Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron," *Boston University Law Review* 81(3) (2001); Ye Diana Wang and Henry H. Emurian, "An Overview of Online Trust: Concepts, Elements, and Implications," *Computers in Human Behavior* 21(1) (2005).

76. Hegghammer, "Interpersonal Trust on Jihadi Internet Forums."

77. Benjamin Ducol, "Uncovering the French-speaking Jihadisphere," pp. 58–59; Jan Marco Leimeister and Helmut Krcmar, "Acceptance and Utility of a Systematically Designed Virtual Community for Cancer Patients," in Peter Van Den Besselaar, Giorgio De Michelis, Jenny Preece, and Carla Simone, eds., *Communities and Technologies 2005: Proceedings of the Second Communities and Technologies Conference* (Dordrecht: Springer, 2005), 140–141; Roger Silverstone, *Media, Technology and Everyday Life in Europe: From Information to Communication* (Aldershot: Ashgate, 2005), pp. 66–70.

78. *The ISIS Twitter Census*, p. 29.

79. Ibid., p. 25.

80. Mia Bloom, "In Defense of Honor: Women and Terrorist Recruitment on the Internet," *Journal of Postcolonial Cultures and Societies* 4(1) (2013); Carolyn Boyle, Alexandra Bradford, and Ross Frenett, *Becoming Mulan: Female Western Migrants to ISIS* (London: Institute for Strategic Dialogue, 2015); Tammy Castle and Meagan Chevalier, "The Women of Stormfront: An Examination of White Nationalist Discussion Threads on the Internet," *Internet Journal of Criminology* (2011). Available at http://www.internetjournalofcriminology.com/Castle_Chevalier_The_Women_of_Stormfront_An_Examination_of_White_Nationalist_Discussion_Threads.pdf (accessed 27 March 2015); Anita Peresin, "Fatal Attraction: Western Muslimas and ISIS," *Perspectives on Terrorism* 9(3) (2015); Erin Marie Saltman and Melanie Smith, *"Till Martyrdom Do Us Part": Gender and the ISIS Phenomenon* (London: Institute for Strategic Dialogue, 2015); Philip Seib and Dana M. Janbek, *Global Terrorism and New Media: The Post-al-Qaeda Generation* (London and New York: Routledge, 2011), ch. 5.
81. Ducol, "Uncovering the French-Speaking Jihadisphere," pp. 54–55.
82. Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), p. 112.
83. Charlie Winter's translation of "Women in the Islamic State" is available at https://www.quilliam foundation.org/wp/wp-content/uploads/publications/free/women-of-the-islamic-state3.pdf
(accessed 30 November 2015). See also Charlie Winter, "Women of The Islamic State: Beyond the Rumor Mill," Jihadology.net 31 March 2015. Available at http://jihadology.net/2015/03/31/guestpost-women-of-the-islamic-state-beyond-the-rumor-mill/ (accessed 26 April 2015).
84. Hoyle et al., *Becoming Mulan?*, p. 32.
85. See, for example, Amy S. Bruckman, "Gender Swapping on the Internet," in Peter Ludlow, ed., *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace* (Cambridge, MA: MIT Press, 1996); Susan C. Herring, "Gender and Power in Online Communication," Center for Social Informatics (CSI) Working Paper No. WP-01-05 (2001). Available at https://scholarworks.iu.edu/dspace/bitstream/handle/2022/1024/WP01-05B.html (accessed 26 April 2015); Zaheer Hussain and Mark D. Griffiths, "Gender Swapping and Socializing in Cyberspace: An Exploratory Study," *CyberPsychology and Behavior* 11(1) (2008); Rosa Mikeal Martey et al., "The Strategic Female: Gender-switching and Player Behavior in Online Games," *Information, Communication & Society* 17(3) (2014); Lynne D. Roberts and Malcolm R. Parks, "The Social Geography of Gender-Switching in Virtual Environments on the Internet," *Information, Communication & Society* 2(4)(1999).
86. Adam Bermingham et al., "Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation," pp. 234–235.
87. Martey et al., "The Strategic Female."
88. ADL, *Computerized Networks of Hate*.