The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research

Ryan Scrivens, Michigan State University
Paul Gill, University College London
Maura Conway, Dublin City University

Abstract:

Many researchers, practitioners, and policy-makers continue to raise questions about the role of the Internet in facilitating violent extremism and terrorism. A surge in research on this issue notwithstanding, relatively few empirically-grounded analyses are yet available. This chapter provides researchers with five key suggestions for progressing knowledge on the role of the Internet in facilitating violent extremism and terrorism so that we may be better placed to determine the significance of online content and activity in the latter going forward. These five suggestions relate to: (1) collecting primary data across multiple types of populations; (2) making archives of violent extremist online content accessible for use by researchers and on user-friendly platforms; (3) outreaching beyond terrorism studies to become acquainted with, for example, the Internet studies literature and engaging in interdisciplinary research with, for example, computer scientists; (4) including former extremists in research projects, either as study participants or project collaborators; and (5) drawing connections between the on- and offline worlds of violent extremists.

Introduction

Like most of us, violent extremists often leave a digital footprint behind. Notable examples include Anders Breivik, the Norwegian far-right terrorist who was a registered member of a white supremacy web-forum (Bartlett and Littler 2011); Dylann Roof, who allegedly posted messages on a white power website (Southern Poverty Law Center 2015); and Aaron Driver, who showed outright support for the so-called 'Islamic State' (IS) on several social media platforms (Amarasingam 2016). In such cases, questions often surround the impact of the offenders' consumption of and networking around violent extremist online content in their up-take of extremist ideology and/or their decision to engage in violent extremism and terrorism.

These questions sit at the top of the priority list for many researchers, practitioners, and policy-makers (Conway 2016). At recent specialized terrorism conferences – including, for example, the 2018 VOX-Pol Conference on 'Violent Extremism, Terrorism, and the Internet: Present and Future Trends' – the nexus between the on- and offline worlds of violent extremists dominates much of the discussion.[1] Similarly, workshops hosted by law enforcement, the defence community, and similar agencies – such as the Swedish Defence Research Agency's Seminar Day on 'Violent Extremism: Methods, Tools and Techniques for Detecting and Analyzing Violent Extremism' – focus much of their attention on gaining insight into how the online discussions, behaviors and actions of violent extremists can spill over into the offline realm.[2] Similarly, at summits and roundtable discussions, social media companies – including Facebook with their Dangerous Organizations Summit – display concern about their platforms facilitating radical communications which, in a number of instances, has translated into violent offline activity. Others, including policy-makers, are concerned that high and increasing levels of always-on Internet access and the production and wide dissemination of large amounts of violent extremist content online may have violent radicalizing effects (Berger and Strathearn 2013; Carter, Maher, and Neumann 2014; Edwards and Gribbon 2013; Gray and Head 2009; Stenersen 2008). This is, after all, a primary goal of the producers of such content.

---

[1] For more information on the conference, visit: https://www.voxpol.eu/events/vox-pol-third-biennial-conference/.
[2] For more information on the workshop, visit: http://www.it.uu.se/research/arenas/security/security-seminars/ELIAS2.

The abovementioned concerns and interests notwithstanding, little is empirically known about the Internet's role in the facilitation of violent extremism and terrorism (Gill, Corner, Conway, Thornton, Bloom, and Horgan 2017).

Determining the significance of the role of the Internet in contemporary extremism and terrorism is not the goal of this chapter, however; it has a narrower remit. It provides researchers with five key suggestions for progressing knowledge on the role of the Internet in facilitating violent extremism and terrorism so that we may be better placed to determine the significance of the Internet's role in the latter going forward. In what follows, we provide five suggestions that relate to: (1) collecting primary data across multiple types of populations; (2) making archives of violent extremist online content accessible for use by researchers and on user-friendly platforms; (3) outreaching beyond terrorism studies to become acquainted with, for example, the Internet studies literature and engaging in interdisciplinary research with, for example, computer scientists; (4) including former extremists in research projects, either as study participants and/or project collaborators; and (5) drawing connections between the on- and offline worlds of violent extremists. This chapter also draws from and builds on Conway's (2016) six suggestions for progressing research on the intersections of violent extremism and terrorism and the Internet.

Recommendation 1: Collecting Primary Data Across Multiple Types of Populations
Reviews of the terrorism research literature regularly highlight the paucity of original data that inform analyses (Schmid and Jongman 1988; Silke 2001, 2004). In his most recent review of the literature, Silke (2013) noted: "[O]ne feels that a great deal more needs to be done before research is consistently building on past work rather than rehashing old data" (p. 34). Resultantly, as Silke argues, terrorism research has lagged behind analogous fields. The most recent review, however, offers a more positive outlook. Schuurman (2018) analyzed over 3,000 articles published in leading terrorism-specific journals between 2007 and 2016 and found that over half used some form of primary sources. The Society for Terrorism Research (2018) also described the data revolution in terrorism studies as a transition from a data shortage to one of "sufficiency and perhaps even excess" (p. 1).

A systematic review of the scientific knowledge base of factors associated with engagement in terrorism shows a similar improvement in empiricism over time (Desmarais, Simons-Rudolph, Brugh, Schilling, and Hoggan 2017). However, this increase has not been

uniform across the field. Empirical studies examining engagement in violent extremism and terrorism demonstrates the field tends to focus on individual-level risk factors (e.g., socio-demographic characteristics, criminal history, religion and spirituality, work and education, relationship status, mental health), personal experiences, attitudes and beliefs, environmental factors and individual motives. Only 18 studies that met Desmarais et al.'s (2017) stringent systematic review criteria empirically examined the radicalization process. Fewer still, presumably, examined the online radicalization process.

Indeed, Hassan et al. (2018) conducted a systematic review specifically focused on the relationship between the impact of extremist online content and violent radicalization. Eleven studies fit their eligibility criteria. The included quantitative studies involved two cross-sectional analyses with data derived from surveys (Pauwels and Schils 2016) and online discussion forums (Wojcieszak 2010), retrospective studies of those who committed acts of terrorism (Gill et al. 2017) and engaged with radicalizing materials on Twitter (Magdy, Darwish, Abokhodair, Rahimi, and Baldwin 2016), and two with pre/post measures conducted in a lab setting (Lee and Leets 2002; Rieger, Frischlich, and Bente 2013). The included qualitative studies involved focus groups that directly exposed participants to propaganda material (Baines, O'Shaughnessy, Moloney, Richards, Butler, and Gill 2010), interviews and ethnographic work with those previously exposed to radicalizing material as well as former extremists (Drevon 2016; Koehler 2014b; Sikorskaya 2017; von Behr, Reding, Edwards, and Gribbon 2013), and case studies including one examining the computer hard-drives of convicted terrorists (Drevon 2016; von Behr et al. 2013). The studies also looked at how exposure to online materials produced changes in emotion (Baines et al. 2010; Sikorskaya 2017), attitudes (Drevon 2016; Koehler 2014b; Lee and Leets 2002; Magdy et al. 2016; Rieger et al. 2013; von Behr et al. 2013; Wojcieszak 2010) and behavior (Drevon 2016; Gill et al. 2017; Pauwels and Schils 2016).

Other empirical studies, however, not included in Hassan et al.'s (2018) systematic review have involved examinations of what media were found on the computers of convicted terrorists (Holbrook 2017; Holbrook 2019), the volume of media consumed by terrorists (Capellan 2015; Gill, Horgan, and Decker 2014; Gruenewald, Chermak, and Freilich 2013; Horgan, Shortland, Abbasciano, and Walsh 2016; Porter and Kebbell 2011), the interaction between the individual consuming the propaganda and the content of the propaganda itself (Bouzar and Martin 2016), the impact of exposure upon attitudinal affinity with an extremist

cause (Ilardi 2013; Kleinmann 2012; Koehler 2014b; Turpin-Petrosino 2002), the impact of exposure upon mobilization to terrorist engagement (Bazex and Mensat 2016; Klausen, Campion, Needle, Nguyen, and Libretti 2016; Reeser 2011; Riaz and Parvez 2018), the specific manifestations of radicalizing narratives that prompted engagement in terrorism (Abbas and Yigit 2016; Özeren, Sever, Yilmaz, and Sözer 2014; Sieckelinck, Sikkens, van San, Kotnis, and De Winter 2017; van San 2018; Wojcieszak 2009), and the impact of exposure upon mobilization to terrorist behavior (Böckler, Hoffman and Zick 2015; Holbrook and Taylor 2017). Many of these studies involved interviews, surveys, and/or access to police files.

The potential to collect primary data (be it, open-, closed- or researcher generated data) across multiple types of populations (e.g., general public, those with attitudinal affinity, those with radicalized beliefs, and those who committed terrorism) is clearly evident. The emerging evidence base is also pretty clear. Those who are radicalized and/or commit acts of terrorism have generally been exposed to radicalizing content. Exposure to this content leads to affective, emotional, and behavioral change at each stage of the process. Of course, some of these studies have relatively small sample sizes, and are only focused on specific types of terrorists or geographical contexts. The key now is to replicate and build upon this preliminary evidence to give us a sense of not just whether exposure to ideological content in the online environment causes violent extremism, but also *how, in what contexts and for whom*?

Is 'exposure' sufficient whether it is in the virtual or physical world? Does it work differently for different people in different contexts? To unpick the specificity of the 'online' environment, exposure to other materials offline have to be incorporated into research designs. The only study of its type is Turpin-Petrosino (2002) who conducted 567 surveys with secondary school and university-level students. The surveys centered around exposure to hate group propaganda and individual attitudes towards these groups. Respondents reported six different types of contact: print material contact (4%), word-of-mouth contact (3.7%), U.S. mail contact (3.4%), local cable television contact (2.6%), Internet contact (1.8%) and phone contact (1.4%). Levels of support for the ideology also differed across these exposure types. Forty percent of those who received Internet contact self-reported supporting either neo-Nazi Skinhead or Ku Klux Klan (KKK) ideology. Of the six exposure types, the Internet was the third most prolific source in changing people's attitudes – behind word-of mouth contact and phone contact. Given

the large innovations in the immersiveness of the online space since this study was conducted, more replications are necessary.

Recommendation 2: Making Archives of Violent Extremist Online Content Accessible for Researchers

The increased attention from researchers to violent extremism and terrorism may be due, in part, to sophisticated, relatively user-friendly, virtual and open-source platforms containing qualitative and/or quantitative data on terrorism events, groups, and individuals (Bowie 2018; Chermak, Freilich, Parkin, and Lynch 2012). These range from academic, think tank and independent databases to commercial and government databases (Bowie 2018). Notable leaders include the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and their Global Terrorism Database (GTD), Profiles of Individual Radicalization in the United States (PIRUS), Profiles of Perpetrators of Terrorism in the United States' (PPT-US), the Terrorist and Extremist Organizations (TEO) Database, and the United States Extremist Crime Database (ECDB); the Pew Research Center's Data Surveys on Terrorism; the Terrorism Research and Analysis Consortium (TRAC) Database; the Southern Poverty Law Center's Extremist Files Database; and the Jihadology online portal (for a recent list of terrorism databases and datasets, see Bowie 2018).

These sources provide unprecedented opportunity and ability to address previously unexplorable questions as well as assess and re-evaluate old research questions with new resources and new research methods. Despite these recent developments, the ability to build, maintain, and make accessible archives of violent extremist online content for use by researchers lags behind parallel fields of study utilizing similar online material (Conway 2016).

Providing researchers with access to non-traditional data sources, especially open source intelligence and social media data, will, without a doubt, transform the future understanding of violent extremism and terrorism in general (LaFree and Freilich 2018) and the role of the Internet in the facilitation of violent extremism and terrorism in particular (Conway 2016). Surprisingly, only a small number of individuals have contributed to this initiative. The University of Arizona's Dark Web Forum Portal, for example, collected and made available the content of 28 jihadi forums comprising nearly 13 million messages.[3] The Dark Crawler (TDC)

---

[3] For more information on the Dark Web Forum Portal, visit https://www.azsecure-data.org.

database, housed at Simon Fraser University (SFU) in Canada, includes – but is not limited to – over 11 million posts from the most conspicuous right-wing extremist forum, Stormfront; over 8 million posts that include Islamist content; as well as over 49 million posts drawn from 11 extreme right-wing subreddits. All are available to users for research upon request.[4] Yet not only are these excellent databases few and far between, these two resources have not been widely used by researchers (some notable exceptions include Chen 2012; Macnair and Frank 2018; Scrivens, Davies and Frank 2017; Scrivens, Davies, and Frank 2018).

What, then, explains the lack of uptake? And why, compared to those who developed the GTD, for example, are so few researchers developing similar databases for the purpose of sharing violent extremist online content with others in the field? For the former, it may be the case that such data sources are much less known than the GTD, for example. For the latter, we suggest it is because most researchers in terrorism studies are social scientists and thus do not have the necessary skills to easily collect, store, and analyze truly large quantities of online data. Further, a lack of standards related to online research, including the absence of methodological rigor related to sampling and concerns about data saturation, plays a role. There are at least four ways to overcome this obstacle however: (1) learn how to undertake basic online data collection and analysis ourselves; (2) build data archives and develop bespoke tools; (3) use commercial data brokers, and; (4) work with computer scientists. Collaborating with colleagues from other disciplines, including computer science, is addressed in the next section, so we will briefly address points 1-3 here.

It is possible 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.[5] Another option, as we have noted above, is to build, maintain, and make accessible archives of violent extremist online content for use by researchers. Wide take-up of these resources will most likely require the availability of easy-to-use analysis tools alongside data in an integrated service, however.

---

[4] For more information on the DarkCralwer, visit https://thedarkcrawler.com.
[5] See, for example, the University of Amsterdam's Digital Methods Initiative at https://www.digitalmethods.net.

The responsibility for sharing accessible content should not only be placed on researchers. Social media companies should take active steps in assisting. This is not a simple undertaking. To illustrate, Twitter has allowed researchers to extract data from their platform using computer programs, but Facebook recently locked down their data following the Cambridge Analytica scandal,[6] making it increasingly difficult for researchers to extract and, by extension, conduct large-scale analyses of Facebook's content (see Bastos and Walker 2018). This is problematic for those working in terrorism studies since Facebook is by far the most popular social networking site in the world (Statista 2018), and widely exploited by violent extremist movements of different ideological standpoints (Awan 2017; Ekman 2018; Johnson et al. 2016; Nouri, Lorenzo-Dus, and Di-Cristofaro 2017; Stier, Posch, Bleier, and Strohmaier 2017; Weimann 2010). While we acknowledge that social media companies must balance the privacy of its users with national security, there requires the development of new partnerships with researchers for the purposes of making online content accessible for scientific purposes. We are seeing some signs of these next steps with, as an example, the implementation of 'Social Science One', an initiative being developed at Harvard University's Institute for Quantitative Social Science in which academics from around the world are working with Facebook to identify valuable datasets that will be made available to researchers through a peer-review process (Reuell 2018).

We further suggest that, in developing industry-academic partnerships in terrorism studies, researchers and social media companies should avoid operating in silos and, by extension, hoarding data. This tactic has historically been the way in which many experts "do business" (see King and Persily 2018). Not sharing information is particularly concerning in this realm given the oftentimes scattered, fragmented nature of data. To illustrate, one stakeholder may have one critical piece of information about the online activity of a particular violent extremist group, for example, while another stakeholder may have another piece of information. Developing open lines of communication and sharing information with researchers will, undeniably, transform our understanding of the role of the Internet in the facilitation of violent extremism and terrorism.

---

[6] In early 2018, it was revealed that personal profiles of approximately 50 million Facebook users was harvested, without their consent, by Cambridge Analytica for political purposes (Bastos and Walker 2018).

In addition to sharing data amongst key stakeholders, those working in this area should make a concerted effort to triangulate data across databases and datasets. Taking a lead in this respect are, for example, Chermak and Holt, who have triangulated data between the ECDB and the PIRUS databases, testing whether theories of social control and social learning shed light on the on- and offline pathways to hate and extremist violence. This provided multiple observational points to explore the similarities and differences across offenders' background, attitudes, and behavior.[7] Perhaps equally valuable would be for researchers to merge such databases (and others) with databases that include violent extremist online content, such as the abovementioned Dark Web Forum Portal and the Dark Crawler database, and develop a central database in which various online platforms that violent extremists and terrorists have been known to frequent can be made available in one space. This would place researchers in a better position to explore, for example, whether consumption of violent extremist online content lead directly to violent acts occurring that would not have occurred if the Internet did not exist.

Recommendation 3: Outreaching Beyond Terrorism Studies and Engaging in Interdisciplinary Research

The original interest of most of those currently researching the intersections of violent extremism and the Internet is the former, rather than the latter. This is easily amendable 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 Jackson (2012) asked about conflict analysis and peace research and its relationship to terrorism studies. He inquired:

How is it 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

---

[7] For more information on this project, visit https://external.ojp.usdoj.gov/SelectorServer/awards/pdf/award/2015-ZA-BX-0004/2016-91422-MD-IJ/2016.

"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 (p. 12)?

Reformulating Jackson's (2012) 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 science 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.

We 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 (Bowen and Bowen 2015; Bryce and Fraser 2014; Naquin and Paulson 2003; Nissenbaum 2011; Wang and Emurian 2005). Hegghammer's (2014) analysis of jihadi online forums is clearly enriched by his drawing from this specific literature, but few other terrorism researchers have followed his lead. Another pertinent area of Internet research is the strongly consistent finding that discussion forums and other online spaces are generally dominated by a few "super contributors" (e.g., Ducol 2012; Leimeister and Krcmar 2005; Silverstone 2005). Berger and Morgan (2015) made a similar finding for IS-related Twitter activity (i.e., of the network of 40,000+ user accounts analyzed, c. 1,500-3,000 were prolific tweeters), 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. 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 did 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, is distinctly different than drawing from other social science fields like communication studies or Internet studies. It was suggested above that social scientists educate ourselves in the use of basic online data collection and analysis tools. However, 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 the day-to-day workings of online extremism and terrorism. Increased collaboration between social scientists, especially terrorism studies scholars, and computer scientists is the most pressing need, but there are a host of other colleagues we could doubtless also benefit from collaborating with (e.g., criminology, psychology, law, etc.).

Recommendation 4: Including Former Extremists in Research Projects

A growing industry (i.e., research centres, consultancy groups, and government departments) is tackling the problem of violent extremism, both in the "real world" and in cyberspace. Known in academic and government circles as 'countering violent extremism' (CVE), it is largely designed to divert individuals from radicalization to violence using "soft" approaches rather than purely securitized and/or criminal justice responses (Harris-Hogan, Barrelle, and Zammit 2015). Commonly, researchers, practitioners, and policy-makers draw from the insights of former violent extremists and terrorists – colloquially known as "formers." Some researchers, however, have raised concerns about including formers in CVE campaigns, ranging from discussions about their reliability and credibility to questions about whether their inclusion could raise concerns in the public sphere (see RAND Corporation 2017).

By conducting in-depth interviews with former extremists, researchers have gained insight into processes of radicalization to violent extremism (Koehler, 2014a, 2014b; Simi, Sporer, and Bubolz 2016), factors that minimize radicalization to mass casualty violence (Simi and Windisch 2018), and greater comprehension of processes of disengagement from violent

extremism (Barrelle 2015; Bubolz and Simi 2015; Horgan, Altier, Shortland, and Taylor 2017; Simi, Blee, DeMichele, and Windisch 2017; Windisch, Ligon, and Simi 2017). Additionally, researchers generally agree that formers can usefully advise on the development and leveraging of counter-narratives due to their first-hand experience in extremist movements. By extension, they are also more likely to be perceived as credible voices by those who may be attracted to violent extremist groups or radical ideologies (Bjørgo and Horgan 2008; Braddock and Horgan 2016; Briggs and Feve 2013; Jacobson 2010; Macnair and Frank 2017).

In recent years, social media, tech companies and think tanks in particular have been quick to turn to formers to assist in the development of online CVE campaigns. The 'Redirect Method' is one illustration. It combines Google's search advertising algorithms (i.e. AdWord technology) and YouTube's video platform to identity those who are searching for violent extremist content on Google and then expose them to counter-narratives.[8] Former extremists have been involved in this process on at least two fronts: (1) a small group of formers developed the list of targeted search terms, and (2) many of the counter-narratives that have been offered to the target audience feature the stories of formers (see Helmus and Klein 2018).

Other online CVE initiatives that have gained attention in recent years include "Extreme Dialogue", which broadcasts an array of emotive films on Twitter, Facebook, and YouTube, some of which include stories from formers. These films attempt to dispel extremist myths and encourage others to actively consider subjective experiences (Reynolds and Tuck 2016). In addition, formers have served as intervention providers on online CVE campaigns, including the Institute for Strategic Dialogue's (ISD) "One to One" pilot project, in which formers directly messaged an array of individuals Facebook identified as right-wing extremists or Islamists (Davey, Birdwell, and Skellett 2018; Frenett and Dow 2014). Lastly, social media and tech companies (such as Google, Facebook, and YouTube), in partnership with think tanks (e.g., ISD) and CVE companies (e.g., Moonshot CVE), collaborate with former extremists to develop and structure new responses to violent extremism online. Here, formers have been drawn upon to enhance the abovementioned stakeholders' knowledge on ways to counter violent online extremism, ranging from formers being asked to identify and provide insight into content of interest (e.g., hate symbols, keywords and terms) to providing tech companies with insight into what counter-narratives may be effective. All such efforts, although on the surface promising,

---

[8] A dedicated Redirect Method website is at https://redirectmethod.org.

still require a full evaluation of effect size and direction, mechanisms (e.g., an understanding of how these efforts make an effect), moderators (e.g., the contexts in which they work best), implementation burdens, and cost (Bowers, Gill, Morgan, Meiklejohn, and Johnson 2018).

Regardless of the abovementioned developments, and despite an increased focus on the intersection of violent extremism, terrorism and the Internet (e.g., Gill et al. 2017; Freilich and Chermak 2012; Gerstenfeld, Grant, and Chiang 2003; Holt 2012), scholars who are working in the field of violent online political extremism have been much slower to bring formers to the table. An exhaustive search using dedicated academic research databases produced only two studies that interviewed former extremists about their Internet usage when they were involved in extremism. Koehler (2014b), for example, conducted in-depth interviews with German former right-wing extremists, with the focus of the study on the role of the Internet in individual radicalization processes. Overall, the author found that the Internet was the most important driving factors in participants' individual radicalization processes, as it provided members with a space in which they could learn skills that were necessary to access online extremist groups. Koehler also found that the Internet was a central hub for extreme right-wing groups, recruiters, and strategies to influence the radical views and subsequent behavior of others online. Sieckelinck et al. (2017), during their interviews with 34 former extremists (extreme right and jihadist) in Denmark and the Netherlands on their life courses into and out of extremism, also highlighted the key catalytic role of exposure to propaganda online. Following the 9/11 attacks, an individual in their study decided to search online for information about the war in Afghanistan. Viewing this content, the participant claimed, was a key push factor within their radicalization process.

Also worth mentioning here are a small number of studies that interviewed current extremists on their media consumption and radicalization process. Ilardi (2013), for example, conducted interviews with seven Canadian jihadists and found that, in combination with close personal relationships with other extremists, the exposure to extremist literature and media was "decisive in instilling in interviewees the type of beliefs that would lead them to identify with the world of radical Islam" (p. 728). Özeren et al. (2014), in their examination of the recruitment strategies of the Kurdistan Workers' Party (PKK) and Kurdistan Communities Union (KCK) via face-to-face interviews with 42 members, depicted the organizations' various media outlets, including websites, online radio and television, as key to the organization's recruitment strategy.

Lastly, Bazex and Mensat (2016) conducted in-depth interviews with 12 young French jihadists who fought in Syria and were, at the time of the study, in custody for terrorist related offenses. The authors, who also had access to investigation files, noted several individual risk factors including delinquent behaviors, setbacks in personal loving relationships, school failure, variability in religious beliefs, and a lack of protective factors. The study also demonstrated that consumption of radical material on the Internet played a fundamental role in the young jihadists' decisions to go to Syria.

Indeed, these studies provide valuable insight into the Internet's role in facilitating violent extremism and terrorism, but this area of research remains in its infancy. Having said this, in progressing our understanding of the role of the Internet in facilitating violent extremism and terrorism, formers who have experience with, and insight into, the online dynamics of violent extremist movements will play a critical role in future research, whether they serve as participants or act as collaborators on research projects. In particular, in furthering our understanding of the interplay between the Internet and violent extremism and terrorism, researchers should incorporate former extremists into their research strategies by interviewing them about their Internet usage and activities when they were involved in violent extremism.

Questions may include those that relate to:

(1) The types of online platforms they frequented when they were in an extremist group or movement (e.g., websites, discussion forums, blogs, social media sites, etc.);

(2) Online activities they engaged in during their time in an extremist group or movement (e.g., radical content consumption, propagandizing, recruitment, networking, planning attacks, etc.);

(3) The extent to which they depended on the Internet to connect and communicate with other adherents when they were in an extremist group or movement;

(4) Their online identity versus offline identity when they were in an extremist group or movement;

(5) The extent to which their online contacts—versus their in-person contacts—influenced their radical belief system during their time in a group or movement; and

(6) The extent to which their online contacts—versus their in-person contacts—influenced their radical behavior and offline activities during their time in a group or movement.

Asking former extremists such questions should provide researchers with first-hand accounts of, and insider's perspectives into, a number of key issues that academics continue to be concerned with, including how the online discussions, behaviors and actions of violent extremists and terrorists can spill over into the offline realm. Within this context, Scrivens et al. (2018) suggest that researchers can assess the potential confluence or divergence of on- and offline behavior by interviewing former extremists who were: (a) active only online; (b) active only offline; and (c) active across both online and off. Comparing their posting behaviors over time may provide much-needed insight into how online behaviors may translate into the offline world.

For formers who are collaborators with researchers on academic projects, researchers may consider including them in decision-making processes, especially at the front end of a project. Formers, for example, can help make decisions about the types of online spaces that should be the focus of a study (e.g., web-forums versus social media platforms) and/or the online content that should be the focus of analysis (e.g., discussions about certain adversary groups, martyrs, religious figures, etc.). At the analysis phase, formers can provide researchers with an in-depth understanding of the online material and inner-workings of particular violent extremist groups, for example. We caution researchers in this regard though. This type of collaboration requires formers who are willing to work with researchers, as well as a level of trust between the two. At the onset of a project, then, both parties should discuss their expectations from the collaboration, especially those that relate to protecting the identity of the former(s). Certainly, formers, out of fear of repercussions by members of their former extremist group (or other groups), may not want to have a public profile and researchers must therefore protect their identities if formers so choose (Briggs and Feve 2013; RAND Corporation 2017). Overcoming these obstacles, and many others not mentioned here (for more information on the challenges of working with formers, see RAND Corporation 2017), will be essential for the development of these collaborations.

Recommendation 5: Drawing Connections Between the On- and Offline Worlds of Violent Extremists

Online radicalization to violence does not happen in a vacuum. Even in those rare cases where all exposure to radicalizing narratives and interactions with other co-ideologues happen in the online space, the individual is still influenced by a crystallization of motives, needs and drivers

from the offline world. In fact, the adoption of extreme beliefs is often a response to other problems in the offline world (see Gill 2015).

To date, we know very little about how this interacts empirically. What little evidence does exist suggests that we should not conceive radicalization as an offline versus online dichotomy. Von Behr et al. (2013), for example, examined primary data of 15 radicalized individuals, nine of whom were convicted under United Kingdom (U.K.) terrorism legislation. The study made use of interviews (with police and the individuals themselves), trial records and computer registries. One key finding suggested the Internet is "not a substitute for in-person meetings but, rather, complements in-person communication" (p. xii).

Additionally, Gill and Corner (2015) looked at the behavioral underpinnings of lone-actor terrorists since 1990. The results suggested that whilst the number of lone-actor terrorist plots remained stable over time, the growth in the Internet has altered their means of radicalization and attack learning. The Internet therefore acts as a substitute for other factors such as intelligence gathering and attack planning, not necessarily a force enabler. Furthermore, according to Gill and Corner, there was a significant positive correlation between those who virtually interacted with co-ideologues and those who interacted with co-ideologues face-to-face.

Building on Gill and Corner (2017), Gill et al. (2017) examined the online behaviors of 223 convicted U.K.-based terrorists. Those who learned online were 4.39 times more likely than those who did not learn online to have experienced non-virtual network activity and 3.17 times more likely to have experienced non-virtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely than those who did not attend training camps to have learned online. Additionally, the evidence also suggested that communicating with co-ideologues online was significantly more likely to have been accompanied by face-to-face interactions with non-violent co-ideologues. Those who communicated online were 3.89 times more likely to have experienced non-virtual network activity and 3.17 times more likely to have experienced non-virtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely to have communicated online. This may be due to the compartmentalization of tasks noted by Gill (2015). For example, individuals tended to learn about a specific necessary task online (e.g., bomb-making), but then found a different instrumentalization in their offline interactions with co-ideologues (e.g., the justification of bombing a particular target).

Finally, Holbrook and Taylor (2017) focused on pre-arrest media usage of five case studies of U.K.-based terrorist who were thwarted and convicted of offenses under terrorism legislation. The cases consist of a lone dyad, a socially active lone actor, an isolated lone actor, a connected lone actor, and a close-knit, hierarchical group. Holbrook and Taylor address a gap in the literature by focussing on behaviors that occurred before subjects were arrested, rather than relying on a post-arrest narrative that may have been skewed by self-justification. In all five cases, a belief pathway precipitated any operational action where all actors were active participants in the consumption, discussion and distribution of extremist materials before any physical involvement in attack planning. Subjects consumed a diverse range of media across a number of platforms and interacted online in chatrooms as well as offline by copying compact discs (CDs) of extremist content for one another.

While much has been learned from these few studies about the link between the on- and offline worlds of violent extremists and terrorism, researchers – in addition to the suggestions described above – should draw from mixed methods approaches to further our understanding of the intersection of violent extremism, terrorism, and the Internet. Researchers, for example, could combine online data with offline data in an effort to triangulate the offline experiences of violent extremists with their online presentation of self, language, and behavior. This, amongst other research strategies, would provide researchers with a more in-depth understanding of the interactions between the on- and offline worlds of violent extremists.

Conclusion

In closing, and by way of full disclosure, we believe the Internet is playing significant and diverse roles in contemporary violent extremism and terrorism. Rapoport (2002) 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, and television) 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 into account: 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, and 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— we 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 (see Anti-Defamation League 1985), but the vast bulk only began to be produced in the 2000s, with a significant uptick since c.2010 and a particular spike since the height of IS. 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 were not possible to address in this article, such as widening the range of types of violent online extremism being studied beyond violent jihadis; engaging in more comparative research, not just across ideologies, but also groups, countries, languages, and social media platforms; deepening our analyses to include interviewing and virtual ethnographic approaches; and paying more attention to gender as a factor in violent online extremism (for more on these, see Conway 2016). Regardless, the purpose of this chapter was to make five 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.

References

Abbas, T., and Yigit, I. H. (2016). Perspectives on Ethno-National Conflict Among Kurdish Families with Members in the PKK. *Terrorism and Political Violence, 28*(2), 297-315.

Amarasingam, A. (2016, August 11). What Aaron Told Ne: An Expert on Extremism Shares His Conversations with the Terror Suspect. *National Post*. Available at https://nationalpost.com/news/canada/what-aaron-told-me-an-expert-on-extremism-shares-his-conversations-with-the-terror-suspect

Anti-Defamation League. (1985). *Computerized Networks of Hate: An ADL Fact Finding Report*. Available at https://archive.org/details/ComputerizedNetworksOfHate

Awan, I. (2017). Cyber-extremism: ISIS and the Power of Social Media. *Social Science and Public Policy, 54*, 138-149.

Baines, P. R., O'Shaughnessy, N. J., Moloney, K., Richards, B., Butler, S., and Gill, M. (2010). The Dark Side of Political Marketing: Islamist Propaganda, Reversal Theory and British Muslims. *European Journal of Marketing, 44*(3/4), 478-495.

Barrelle, K. (2015). Pro-Integration: Disengagement from and Life After Extremism. *Behavioral Sciences of Terrorism and Political Aggression, 7*(5), 129-142.

Bartlett, J., and Littler, M. (2011). Insight the EDL: Populist Politics in the Digital Era. *Demos*. Available at https://www.demos.co.uk/files/Inside_the_edl_WEB.pdf?1331035419

Bastos, M., and Walker, S. T. (2018). Facebook's Data Lockdown is a Disaster for Academic Researchers. *The Conversation*. Available at https://theconversation.com/facebooks-data-lockdown-is-a-disaster-for-academic-researchers-94533

Bazex, H., and Mensat, J-Y. (2016). Who are the French Jihadists? Analysis of 12 Cases to Help Develop Profiles and Assessment of the Risk of Acting Out. *Annales Medico-Psychologiques, 174*(4), 257-265.

Berger, J. M., and Morgan, J. (2015). *The ISIS Twitter Census*. Brookings Institution.

Berger, J. M., and Strathearn, B. (2013). *Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Extremism in Online Social Networks*. King's College London: International Centre for the Study of Radicalisation and Political Violence.

Böckler, N., Hoffmann, J., and Zick, A. (2015). The Frankfurt Airport Attack: A Case Study on the Radicalization of a Lone-Actor Terrorist. *Journal of Threat Assessment and Management, 2*(3-4), 153-163.

Bouzar, D., and Martin, M. (2016). Pour quels motifs les jeunes s' engagent-ils dans le djihad? *Neuropsychiatrie de l'Enfance et de l'Adolescence, 64*(6), 353-359.

Bowen, G., and Bowen, R. (2015). Brand Trust in Offline and Online Environments: Lessons for Social Media. In G. Bowen and W. Ozue (Eds.), *Computer-Mediated Marketing Strategies: Social Media and Online Brand Communities* (pp. 58-82). Hershey, PA: IGI Global.

Bowers, K., Gill, P., Morgan, P., Meiklejohn, S., and Johnson, S. (2018). Challenges for EMMIE as a Realist Evaluation Framework. In G. Farrell and A. Sidebottom (Eds.), *Realist Evaluation for Crime Science: Essays in Honour of Nick Tilley* (pp. 98-118). London: Routledge.

Bowie, N. G. (2018). 30 Terrorism Databases and Data Sets: A New Inventory. *Perspectives on Terrorism, 12*(5), 51-61.

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

Briggs, R., and Feve, S. (2013). *Review of Programs to Counter Narratives of Violent Extremism: What Works and What are the Implications for Government*. London: Institute for Strategic Dialogue.

Bryce, J., and Fraser, J. (2014). The Role of Disclosure of Personal Information in the Evaluation of Risk and Trust in Young Peoples' Online Interactions. *Computers in Human Behavior, 30*, 299-306.

Bubolz, B. F., and Simi, P. (2015). Leaving the World of Hate: Life-Course Transitions and Self-Change. *American Behavioral Scientist, 59*(12), 1588-1608.

Capellan, J. A. (2015). Lone Wolf Terrorist or Deranged Shooter? A Study of Ideological Active Shooter Events in the United States, 1970-2014. *Studies in Conflict and Terrorism, 38*(6), 395-413.

Carter, J., Maher, S., and Neumann, P. (2014). *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*. King's College London: International Centre for the Study of Radicalisation and Political Violence.

Chen, H. (2012). *Dark Web: Exploring and Data Mining the Dark Side of the Web*. New York: Springer.

Chermak, S. M., Freilich, J. D., Parkin, W. S., and Lynch, J. P. (2012). American Terrorism and Extremist Crime Data Sources and Selectivity Bias: An Investigation Focusing on Homicide Events Committed by Far-Right Extremists. *Journal of Quantitative Criminology, 28*, 191-218.

Conway, M. (2016). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict and Terrorism, 40*(1), 77-98.

Davey, J., Birdwell, J., and Skellett, R. (2018). *Counter Conversations: A Model for Direct Engagement with Individuals Showing Signs of Radicalization Online*. London: Institute for Strategic Dialogue.

Desmarais, S. L., Simons-Rudolph, J., Brugh, C. S., Schilling, E., and Hoggan, C. (2017). The State of Scientific Knowledge Regarding Factors Associated with Terrorism. *Journal of Threat Assessment and Management, 4*(4), 180-209.

Drevon, J. (2016). Embracing Salafi Jihadism in Egypt and Mobilizing in the Syrian Jihad. *Middle East Critique, 25*(4), 321-339.

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

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

Ekman, M. (2018). Anti-Refugee Mobilization in Social Media: The Case of Soldiers of Odin. *Social Media and Society, 4*(1), 1-11.

Freilich, J. D., and Chermak. S. M. (2012). Terrorists use of the Internet: An Analysis of Strategies, Objectives and Law Responses. In H. S. Yoon (Ed.), *Cyberterrorism: Trends and Responses* (pp. 133-167). Seoul, South Korea: Korean Institute of Criminology.

Frenett, R., and Dow, M. (2014). *One to One Interventions: A Pilot CVE Methodology*. London: Institute for Strategic Dialogue and Curtain University.

Gerstenfeld, P. B., Grant, D. R., and Chiang, C-P. (2003). Hate Online: A Content Analysis of Extremist Internet Sites. *Analyses of Social Issues and Public Policy, 3*(1), 29-44.

Gill, P. (2015). *Lone-Actor Terrorists: A Behavioural Analysis*. London: Routledge.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., and Horgan J. (2017). Terrorist use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes. *Criminology and Public Policy, 16*(1), 99-117.

Gill, P., and Corner, E. (2015). Lone-Actor Terrorist use of the Internet and Behavioural Correlates. In L. Jarvis, S. Macdonald, and T. M. Chen (Eds.), *Terrorism Online: Politics, Law, Technology and Unconventional Violence* (pp. 35-53). London: Routledge.

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

Gray, D. H., and Head, A. (2009). 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), 396-404.

Gruenewald, J., Chermak, S., and Freilich, J. D. (2013). Distinguishing "Loner" Attacks from Other Domestic Extremist Violence: A Comparison of Far-Right Homicide Incident and Offender Characteristics. *Criminology and Public Policy, 12*(1), 65-91.

Harris-Hogan, S., Barrelle, K., and Zammit, A. (2015). What is Countering Violent Extremism? Exploring CVE Policy and Practice in Australia. *Behavioral Sciences of Terrorism and Political Aggression, 8*(1), 6-24.

Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., ... and Sieckelinck, S. (2018). Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence. *International Journal of Developmental Science, 12*(1-2), 71-88.

Hegghammer, T. (2014). *Interpersonal Trust on Jihadi Internet Forums*. Available at http://hegghammer.com/_files/Interpersonal_trust.pdf.

Helmus T. C., and Klein, K. (2018). *Assessing Outcomes of Online Campaigns Countering Violent Extremism: A Case Study of the Redirect Method*. Santa Monica, CA: RAND Corporation.

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime and Terror. *Terrorism and Political Violence, 24*(2), 337-354.

Holbrook, D. (2017). What Types of Media do Terrorists Collect? *International Centre for Counter-Terrorism Research Paper*. Available at https://icct.nl/wp-

content/uploads/2017/09/ICCT-Holbrook-What-Types-of-Media-Do-Terrorists-Collect-Sept-2017-2.pdf

Holbrook, D. (2019). The Terrorism Information Environment: Analysing Terrorists' Selection of Ideological and Facilitative Material. *Terrorism and Political Violence*. Ahead of Print.

Holbrook, D., and Taylor, M. (2017). Terrorism as Process Narratives: A Study of Pre-Arrest Media Usage and the Emergence of Pathways to Engagement. *Terrorism and Political Violence*. Ahead of Print.

Horgan, J., Altier, M. B., Shortland, N., and Taylor, M. (2017). Walking Away: The Disengagement and De-Radicalization of a Violent Right-Wing Extremist. *Behavioral Sciences of Terrorism and Political Aggression, 9*(2), 63-77.

Horgan, J., Shortland, N., Abbasciano, S., and Walsh, S. (2016). Actions Speak Louder Than Words: A Behavioral Analysis of 183 Individuals Convicted for Terrorist Offenses in the United States from 1995 to 2012. *Journal of Forensic Sciences, 61*(5), 1228-1237.

Ilardi, G. J. (2013). Interviews with Canadian Radicals. *Studies in Conflict and Terrorism, 36*(9), 713-738.

Jackson, R. (2012). Unknown Knowns: The Subjugated Knowledge of Terrorism Studies. *Critical Studies on Terrorism, 5*(1), 11-29

Jacobson, M. (2010). Terrorist Drop-Outs: One Way of Promoting a Counter-Narrative. *Perspectives on Terrorism, 3*(2), 12-17.

Johnson, N. F, Zheng, M., Vorobyeva, Y., Gabriel, A., Qi, H., Velasquez, N., ... and Wuchty, S. (2016). New Online Ecology of Adversarial Aggregates: ISIS and Beyond. *Science, 352* (6292), 1459-1463.

King, G., and Persily, N. (2018). A New Model for Industry-Academic Partnerships. *Working Paper.* Available at https://gking.harvard.edu/files/gking/files/partnerships.pdf

Klausen, J., Campion, S., Needle, N., Nguyen, G., and Libretti, R. (2016). Toward a Behavioral Model of "Homegrown" Radicalization Trajectories. *Studies in Conflict and Terrorism, 39*(1), 67-83.

Kleinmann, S. M. (2012). Radicalization of Homegrown Sunni Militants in the United States: Comparing Converts and Non-converts. *Studies in Conflict and Terrorism, 35*(4), 278-297.

Koehler, D. (2014a). Right-Wing Extremist Radicalization Processes: The Formers' Perspective. *JEX Journal EXIT-Deutschland, 1*, 307-377.

Koehler, D. (2016b). The Radical Online: Individual Radicalization Processes and the Role of the Internet. *Journal for Deradicalization, 1*, 116-134.

LaFree, G., and Freilich, J. D. (2018). Government Policies for Counteracting Violent Extremism. *Annual Review of Criminology, 2*, 383-404.

Lee, E., and Leets, L. (2002). Persuasive Storytelling by Hate Groups Online: Examining Its Effects on Adolescents. *American Behavioral Scientist, 45*(6), 927-957.

Leimeister, J. M., and Krcmar, H. (2005). Acceptance and Utility of a Systematically Designed Virtual Community for Cancer Patients. In P. Van Den Besselaar, G. De Michelis, J. Preece, and C. Simone, (Eds.), *Communities and Technologies 2005: Proceedings of the Second Communities and Technologies Conference* (pp. 129-148). Dordrecht: Springer.

Magdy, W., Darwish, K., Abokhodair, N., Rahimi, A., and Baldwin, T. (2016). #ISISisNotIslam or #DeportAllMuslims? Predicting Unspoken Views. In *Proceedings of the 8th ACM Conference on Web Science*, Hannover, Germany, pp. 95-106.

Macnair, L., and Frank, R. (2017). Voices Against Extremism: A Case Study of a Community-Based CVE Counter-Narrative Campaign. *Journal for Deradicalization, 10*, 147-174.

Macnair, L., and Frank, R. (2018). The Mediums and the Messages: Exploring the Language of Islamic State Media through Sentiment Analysis. *Critical Studies on Terrorism, 11*(3), 438-457.

Naquin, C. E., and Paulson, G. D. (2003). Online Bargaining and Interpersonal Trust. *Journal of Applied Psychology, 88*(1), 113-20.

Nissenbaum, H. (2001). Securing Trust Online: Wisdom or Oxymoron. *Boston University Law Review, 81*(3), 635-664.

Nouri, L., Lorenzo-Dus, N., and Di-Cristofaro, M. (2017). *Extreme Far Right Groups' Use of Social Media: A Focus on Britain First and Reclaim Australia*. Swansea, UK: Cyberterrorism Project Research Report (No. 7).

Özeren, S., Sever, M., Yilmaz, K., and Sözer, A. (2014). Whom Do They Recruit? Profiling and Recruitment in the PKK/KCK. *Studies in Conflict and Terrorism, 37*(4), 322-347.

Pauwels, L., and Schils, N. (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.

Porter, L. E., and Kebbell, M. R. (2011). Radicalization in Australia: Examining Australia's Convicted Terrorists. *Psychiatry, Psychology and Law, 18*(2), 212-231.

RAND Corporation. (2017). *Dos and Don'ts of Involving Formers in PVE/CVE Work*. Available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/dos_and_donts_involving_formers_in_pve_cve_work_bordeaux_27_06_2017_en.pdf

Rapoport, D. (2002). The Four Waves of Rebel Terror and September 11. *Anthropoetics 8*(1).

Reeser, A. M. S. (2011). *The Tipping Point to Terrorism: Involvement in Right-Wing Terrorist Groups in the United States*. Ph.D. Thesis. Available at https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1034andcontext=studentwork

Reuell, P. (2018). Organization Set to Release Massive Trove of Information, Strictly for Research Purposes. *The Harvard Gazette*. Available at https://news.harvard.edu/gazette/story/2018/07/mining-facebook-data-for-science/

Reynolds, L., and Tuck, H. (2016). *The Counter-Narrative Monitoring and Evaluation Handbook*. London: Institute for Strategic Dialogue.

Riaz, A., and Parvez, S. (2018). Bangladeshi Militants: What Do We Know? *Terrorism and Political Violence, 30*(6), 944-961.

Rieger, D., Frischlich, L., and Bente, G. (2013). *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*. Cologne: Wolters Kluwer.

Schmid, A. P., and Jongman, A. J. (1988). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. New Brunswick, NJ: Transaction Books.

Schuurman, B. (2018). Research on Terrorism, 2007-2016: A Review of Data, Methods, and Authorship. *Terrorism and Political Violence.* Ahead of Print.

Scrivens, R., Davies, G., and Frank, R. (2017). Searching for Signs of Extremism on the Web: An Introduction to Sentiment-based Identification of Radical Authors. *Behavioral Sciences of Terrorism and Political Aggression, 10*(1), 39-59.

Scrivens, R., Davies, G., and Frank, R. (2018). Measuring the Evolution of Radical Right-Wing Posting Behaviors Online. *Deviant Behavior*. Ahead of Print.

Sieckelinck, S., Sikkens, E., van San, M., Kotnis, S., and De Winter, M. (2017). Transitional Journeys Into and Out of Extremism. A Biographical Approach. *Studies in Conflict and Terrorism*. Ahead of Print.

Sikorskaya, I. (2017). *Messages, Images and Media Channels Promoting Youth Radicalization in Kyrgyzstan*. Bishkek, Kyrgyzstan: Search for Common Ground.

Silke, A. (2001). The Devil You Know: Continuing Problems with Research on Terrorism. *Terrorism and Political Violence, 13*(4), 1-14.

Silke, A. (2004). An Introduction to Terrorism Research. In A. Silke (Ed.), *Research on Terrorism: Trends, Achievements and Failures* (pp. 1-29). London: Routledge.

Silke, Andrew. 2013. Research on terrorism: A review of the impact of 9/11 and the global war on terrorism. In Adam Dolnik (ed.), Conducting Terrorism Field Research: A Guide. London: Routledge.

Silverstone, R. (2005). *Media, Technology and Everyday Life in Europe: From Information to Communication*. Aldershot: Ashgate.

Simi, P., Blee, K., DeMichele, M., and Windisch, S. (2017). Addicted to Hate: Identity Residual among Former White Supremacists. *American Sociological Review, 82*(6), 1167-1187.

Simi, P., Sporer, K., and Bubolz, B. F. (2016). Narratives of Childhood Adversity and Adolescent Misconduct as Precursors to Violent Extremism: A Life-Course Criminological Approach. *Journal of Research in Crime and Delinquency, 53*(4), 536-563.

Simi, P, and Windisch, S. (2018). Why Radicalization Fails: Barriers to Mass Casualty Terrorism. *Terrorism and Political Violence*. Ahead of Print.

Society for Terrorism Research. (2018). *STR2019 - Call for Papers*. Available at https://www.sv.uio.no/c-rex/english/news-and-events/news/2018/str2019-call-for-papers.html

Southern Poverty Law Center. (2015). *Dylann Roof may have been a Regular Commenter at Neo-Nazi Website The Daily Stormer*. Available at https://www.splcenter.org/hatewatch/2015/06/21/dylann-roof-may-have-been-regular-commenter-neo-nazi-website-daily-stormer

Statista. (2018). *Most Famous Social Network Sites Worldwide as of October 2018, Ranked by Number of Active Users (in Millions)*. Available at https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Stenersen, A. (2008). The Internet: A Virtual Training Camp? *Terrorism and Political Violence, 20*(2), 215-233.

Stier, S., Posch, L., Bleier, A., and Strohmaier, M. (2017). When Populists Become Popular: Comparing Facebook use by the Right-Wing Movement Pegida and German Political Parties. *Information, Communication and Society, 20*(9), 1365-1388.

Turpin-Petrosino, C. (2002). Hateful Sirens…Who Hears Their Song? An Examination of Student Attitudes Toward Hate Groups and Affiliation Potential. *Journal of Social Issues, 58*(2), 281-301.

van San, M. (2018). Belgian and Dutch Young Men and Women Who Joined ISIS: Ethnographic Research Among the Families They Left Behind. *Studies in Conflict and Terrorism, 41*(1), 39-58.

von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013). *Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Santa Monica, CA: RAND Corporation.

Wang, Y. D., and Emurian, H. H. (2005). An Overview of Online Trust: Concepts, Elements, and Implications. *Computers in Human Behavior, 21*(1), 105-125.

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

Windisch, S., Ligon, G. S., and Simi, P. (2017). Organizational [Dis]trust: Comparing Disengagement Among Former Left-Wing and Right-Wing Violent Extremists. *Studies in Conflict and Terrorism*. Ahead of Print.

Wojcieszak, M. (2009). "Carrying Online Participation Offline"—Mobilization by Radical online Groups and Politically Dissimilar Offline Ties. *Journal of Communication, 59*(3), 564-586.

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