PERSPECTIVE | EXPERT INSIGHTS ON A TIMELY POLICY ISSUE
APRIL 2022

HOW EXTREMISM OPERATES ONLINE

A Primer

ALEXANDRA T. EVANS AND HEATHER J. WILLIAMS

RAND CORPORATION

ABOUT RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0840-2

Limited Print and Electronic Distribution Rights

For more information on this publication,
visit www.rand.org/t/PEA1458-2.

Collage illustrations by Jessica Arana

CONTENTS

On May 7, 2021, the United States endorsed the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online, joining a coalition of member governments, international organizations, and private technology companies that have pledged to combat malicious actors' exploitation of the internet.[1] In its announcement, the White House affirmed that "[c]ountering the use of the internet by terrorists and violent extremists to radicalize and recruit is a significant priority for the United States."[2]

The decision, one of a host of new measures targeting online extremist activity that have been enacted or are reported to be under review by the Biden administration, exemplified U.S. policymakers' recognition of the important role that the internet plays in mobilizing, sustaining, and propagating extremist activity.[3] Since the mid-1980s, extremist movements across the ideological spectrum have demonstrated their intent and ability to exploit digital communication, networking, and commerce tools and to transition some of their operations online.[4] These activities began to capture policy attention in the early 2000s, but the challenge has gained new

urgency in recent years as groups and movements such as the Islamic State in Iraq and Syria (ISIS), the Q-Anon conspiracy theory, and the #StopTheSteal political campaign have harnessed social media and other virtual platforms to generate major real-world effects.[5]

The purpose of this Perspective is to synthesize existing research on how the internet influences the activities of extremist groups and movements and how exposure to or consumption of extremist content online influences the behavior of internet users. We surveyed studies and analyses produced over the past two decades by academics, nongovernmental organizations, and other civil sector entities that have sought to better understand whether new technologies have changed how radical ideas spread, how they gain a hold, and how they motivate people to act on their grievances. The second in a series of RAND Corporation primers on the far-right virtual extremist ecosystem,[6] this Perspective is intended to promote a general understanding of trends in the current literature and to identify areas of emerging consensus, as well as ongoing disagreement and outstanding questions. The information collected here also may be of interest to those looking to improve their ability to recognize, avoid, or resist hateful, violent, and other manipulative online activity.

We have organized this Perspective into four sections. The first provides a brief definition of core terms and notes areas of conceptual disagreement. The second focuses on how the internet enables extremist organizations and movements by facilitating such basic operational functions as fundraising, recruiting, and knowledge transfer. The third focuses on how individuals receive extremist online material, and how the dynamics of the virtual world can facilitate receptivity to extremist ideas and, possibly, offline violence. We conclude with a discussion of research that addresses how the internet can be leveraged as a tool to counter extremism, before outlining avenues for further research that could contribute to the prevention, intervention, and monitoring of harmful activity.

TERMINOLOGY AND SCOPE

The variety (and often the ambiguity) of the language used to describe online extremist activity complicates any attempt to survey the literature. By its nature, extremism is a relative concept whose meaning can shift depending on political and cultural context.[7] Although the term *extremism* appears in federal regulations, grant program descriptions, and policy statements, there exists no statutory definition or intergovernmental standard to guide usage of the term in the United States.[8] (U.S. statutes do, however, define foreign and domestic *terrorism*, and federal agencies maintain a public list of foreign, but not domestic, terrorist groups.) To the contrary, the U.S. government has shied away from universal definitions and has instead advanced a variety of related terms to describe an inexhaustive list of specific extremist movements.[9] Intended to promote clarity and objectivity, these lists have been revised repeatedly over the past several years and have been adopted unevenly across and outside the U.S. government.[10]

Complicating matters further, the U.S. government has begun using the terms *domestic extremism* and *domestic terrorism* interchangeably and without clarifying any distinction between these concepts or their significance.[11] This approach has raised concerns from observers who are worried that the conflation may infringe upon civil liberties or challenge constitutional speech protections.[12] On the other end of the spectrum, failing to specifically label certain movements

(e.g., white separatist and white nationalist movements) as extremist allows them to portray their principles as nonviolent and to insert their rhetoric and proposals into the national discourse.[13]

This fragmentation is compounded by the fact that research on virtual extremism spans many disciplines and fields, with scholars of various backgrounds often employing different terminology and methods to describe similar phenomena or to frame related research questions. Some use *extremism* or *extremist* only in reference to movements that advocate the use of violence; others include nonviolent ideologies that advocate criminal activities or fall far outside the political mainstream.[14] The lack of consensus over what constitutes extremism has led some scholars and analysts to reject the term altogether in favor of related concepts, such as *terrorism* and *political violence*, although these terms are also the subject of definitional debates.[15] In other cases, scholars approaching these questions from such fields as constitutional law, information and communication studies, computer science, and human-computer interface design might use field-specific jargon or frameworks that are unfamiliar to scholars whose work concentrates on questions of extremism, terrorism, or hate crimes and racism.

To identify cross-cutting patterns and facilitate analytical comparisons, we used an inclusive definition to identify relevant literature. In the context of this Perspective, the term *extremism* operates as an umbrella concept for related subcategories, such as fanaticism and terrorism, which evoke a common desire or willingness to operate outside established institutions and to use illegal force, threats, or other harmful actions to promote political causes and enact desired changes.[16] Our definition is intended to include groups that advocate a variety of antisocial behaviors, which may include bodily harm, and to exclude subcultures, such as gangs, that do not pursue political aims. Although this review was conducted as part of a larger project that examines the online activity of white supremacists and violent misogynists, we did not limit our survey to works that focus on specific ideologies. To the contrary, we purposefully included research analyzing the online behavior of other extremist movements, such as Sunni radicals. This choice reflects both the fact that most of the literature on extremism published in the past decade has focused on Islamist organizations and the fact that far-right extremist movements observe and learn from major terrorist groups' use of the internet.[17]

HOW EXTREMIST MOVEMENTS AND GROUPS USE THE INTERNET

Beginning in the early 1990s, researchers, government agencies, and civil sector organizations have cataloged how various extremist groups and movements use the internet to replicate, and at times replace, functions previously undertaken in the physical world.[18] These studies have demonstrated how social media, file upload sites, encrypted communication applications, and other internet-based platforms can aid extremist movements by decreasing costs, generating efficiencies, increasing access to new audiences, granting anonymity and other security measures, and otherwise lowering traditional barriers to organizing.

Although the specific strategies for internet use vary among groups and movements, our analysis found that the internet-enabled functions described in the literature generally fall into one of five categories: (1) financing; (2) networking and coor-

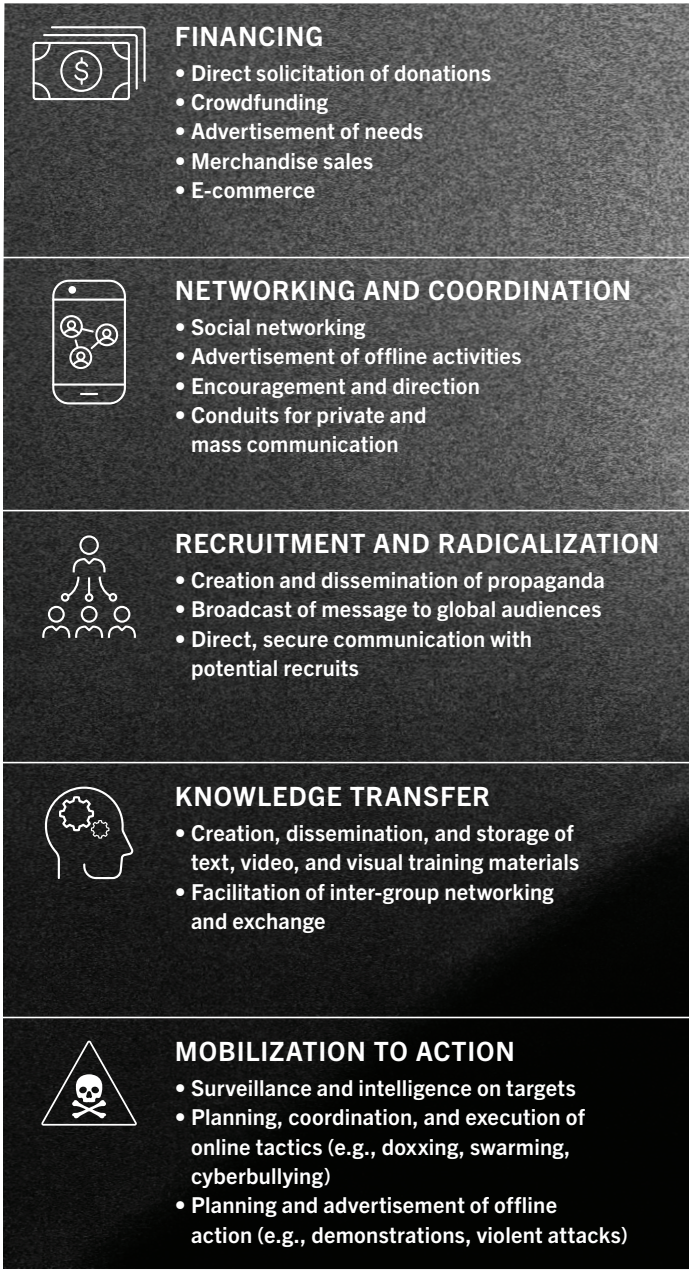
dination; (3) recruitment and radicalization; (4) inter- and intra-group knowledge transfer; and (5) mobilization to action (see Figure 1 for additional details).

Financing and fundraising functions illustrate how extremists can use internet-based tools to mimic activities that are traditionally performed in physical spaces.[19] Websites, social media platforms, email distribution lists, messaging apps, and other virtual tools enable groups to publicize their needs, to direct potential donors to traditional and online payment options, and to advertise merchandise for sale, as they might have done historically using print advertisements and paper flyers.[20] The simplest and perhaps most common method for an organization to solicit funds is by posting requests for donations on its website or on forums where supporters already congregate.[21] Extremist groups have also harnessed crowdfunding websites and donation applications embedded in social media platforms, such as Facebook, to expand their reach and elevate their causes.[22]

Extremist groups may also augment these traditional revenue streams with new forms of e-commerce. Some have used online retail platforms and payment processing architecture to generate funds through merchandise sales conducted directly on their websites or through such intermediaries as eBay, Amazon, and Etsy.[23] Extremists have also profited from self-publishing services (e.g., Amazon's CreateSpace) and from music-streaming services (e.g., Spotify or iTunes) that serve the dual purpose of fundraising and disseminating radical ideas.[24]

Not all extremist individuals or groups engage in these activities. For instance, most far-right attacks have been self-financed by their perpetrators, in part because they required few resources and were conducted through decentralized networks or by individuals acting alone.[25] Yet, for larger

FIGURE 1



groups and movements that seek to conduct more-complex operations, the internet provides a useful and relatively low-risk means to generate the resources required to sustain or expand their activities. These efforts may supplement, rather than replace, traditional fundraising channels based in the physical world, but they are appealing because they provide global reach and afford a degree of anonymity and security to donors and recipients alike.[26]

Similarly, extremists have turned to the internet to manage their human resources. Beginning with the invention of the public bulletin board system in the 1980s, white supremacists, far-right activists, and other extremist actors have used digital communication tools to socialize, network within and among communities, and coordinate online and offline activities.[27] Social media platforms, discussion forums, and information search engines provide new pathways for sympathetic individuals to find or expand their interaction with extremist activists or organizations that maintain public or semipublic profiles.[28] Although researchers disagree over whether online interactions can or will supplant the role of face-to-face relationships, it is clear that recruiters affiliated with groups across the ideological spectrum use internet technologies to identify and assess potential members.[29] The characteristics of virtual interaction—in particular the accessibility and efficiency of digital communication and networking tools—enable the integration of new members into a movement, ease information-sharing, and facilitate participation in both online and offline activities.[30]

The internet's ability to connect geographically distributed users makes it additionally appealing to recruiters—and a cause for concern for international law enforcement and intelligence agencies. For a group like the Islamic State, which sought to both conscript foreign fighters and encourage adherents to launch attacks in place, social media proved an effective tool to identify, vet, enlist, and coordinate the activities of prospective recruits.[31] The internet similarly has offered right-wing extremists with cheap, efficient, and safe means to communicate and network, while providing new ways to create the impression that a movement has attracted a substantial supporter base.[32]

Although the internet's ability to surmount physical distance is part of its attraction, extremists also use social media, encrypted communication channels, and other similar platforms to recruit and organize adherents who live in close proximity but are either unaware of or hesitant to seek out opportunities to interact in the real world. Social networking platforms can encourage or facilitate the creation of offline relationships by connecting socially isolated individuals whose "real world social networks may not engender connections to radical movements" otherwise.[33] A majority of former racist skinheads interviewed for one study described discussion forums, chatrooms, and social media sites as "ideal spaces" to advertise and encourage participation in offline, movement-related activities, and one-third of those interviewed reported that their first face-to-face interactions had been arranged through virtual interactions.[34] "A key feature of online platforms that facilitated the connection with the offline world … was the interactive and localized nature of these spaces," the study's authors found, noting that "the like-minded could seek out, connect and interact with local adherents online who shared their views and who they could then meet in offline, in-person settings."[35] This finding is supported by other research that has demonstrated how social media and other virtual communication tools enhance physical organizing by helping extremists and prospective recruits find, communicate with, and arrange meetings with other like-minded individuals.[36]

If the internet has increased the number of points of entry into a movement, the evidence suggests that it has also facilitated knowledge transfer and coordination on a new scale. The availability of free or low-cost streaming services, file storage platforms, and end-to-end encrypted communication applications has made it easier and faster to share training manuals, ideological tracts, and propaganda across the world.[37] For groups that control territory as the Islamic State did between 2014 and 2017, virtual communication platforms can complement more-traditional means of recruiting and training fighters and spreading their messages.[38] In other cases, terrorist groups may turn to the internet as a temporary solution to compensate for the loss of offline training facilities, such as in the cases of al Qaeda after 2001 and the Islamic State after 2017.[39]

But for the majority of extremist and terrorist groups that either do not control physical territory or employ a leaderless resistance strategy, the internet has emerged as the primary means to acquire and share tactical, operational, and ideological training.[40] As one criminologist notes, "users can instantly download (and disseminate) fliers, books, magazines and newsletters, as well as, watch and listen to recorded or live streaming audio and video in the privacy of their own homes."[41] Like fundraising operations, these activities attract new recruits by conveying the impression that a group controls sensitive or sophisticated training materials and by opening channels to spread other propaganda. For example, far-right and white-supremacist groups have shared operational manuals and training guides online alongside racist biographies, manifestos, and other written works to educate existing group members and to persuade potential or new supporters that their agendas are well established.[42] Other studies have highlighted the Islamic State's persistent use of anonymous file-sharing portals to generate content, disseminate propaganda, and maintain communication networks despite coordinated international efforts to degrade the group's social media operations.[43]

Of course, the internet is not a panacea for all the operational challenges that extremist movements face. Violent extremists still require access to weapons, explosives, or other equipment to conduct physical attacks, and both violent and nonviolent groups continue to conduct some sensitive planning activities face to face. Moreover, virtual income streams may be more susceptible to disruption than their offline antecedents. To build the webpages required to solicit donations, advertise merchandise, and disseminate crowdfunding campaigns—and then to process internet transactions and transfer funds—requires access to a complex network of private companies that control the internet's architecture and facilitate financial interactions. Under public and, at times, governmental pressure, these companies have occasionally revised their acceptable-use guidelines to prohibit or limit the use of their services by extremists.[44]

Likewise, digital networks are susceptible to infiltration or exposure by both law enforcement agencies and political activists.[45] U.S. intelligence agencies, the Federal Bureau of Investigation, and local law enforcement agencies have publicly acknowledged that they surveil electronic communications of suspected criminals and terrorists, and social media posts, emails, and other digital interactions are routinely used to build criminal cases against alleged domestic and international terrorists.[46] In addition, activists on both the left and the right have employed *doxxing* (the practice of revealing, typically online, private or identifying information about a person without their permission) to humiliate, delegitimize, threaten, or otherwise punish members of online extremist

communities.[47] But although anecdotal evidence suggests that the possibility of infiltration or exposure has caused paranoia and distrust within extremist networks, it is unclear whether online networks are more susceptible to infiltration and disruption than their offline counterparts are.[48] Similarly, there is no evidence that doxxing, which a Department of Justice bulletin described as a form of "cyberharassment," produces a net reduction in online extremism, in part because most of the scholarship focuses on perpetrators' intentions and individual harms rather than the practice's broader consequences for a movement.[49]

To date, however, these complications do not appear to have dissuaded extremist groups from conducting at least some of their activities online—in part because the internet continues to provide solutions for these challenges. Major technology companies' attempts to tighten content-moderation policies have spurred mass relocations of users to more-hospitable platforms and have contributed to the creation of a new generation of lenient "alt-technology" platforms that tolerate and, in some cases, openly encourage radical groups to use their services.[50] Emerging internet-based technologies like cryptocurrencies and new forms of peer-to-peer encryption may also provide extremist groups with new ways to lessen their dependence on physical organizing and traditional institutions, although technological and social barriers continue to hinder more widespread adoption.[51] Whether extremists' activity on encrypted communication platforms differs fundamentally from their behavior on open platforms is still unclear, however. Researchers have begun to explore this question in light of the growing popularity and accessibility of free and low-cost commercial tools, but challenges in accessing user and content data remain a significant constraint.[52]

Although specialist communities exist online, the notion of a separate extremist internet is a myth.

For most extremist groups and movements, the internet remains a tool to sustain and expand their operations and to accumulate the support, knowledge, and resources to force political change in the physical world. Although the scale, sophistication, and frequency of extremist virtual activity have changed over time, three general patterns are apparent:

- First, **nearly all extremist movements now engage in some virtual activity**, although the specific nature and extent of internet use varies. In part, this shift is a reflection of the general societal transformation over the past two decades; with the expansion of internet access, virtual interactions have become part of almost every aspect of daily life. But the expansion in online extremist activity is also a testament to the demonstrated utility of the internet in enabling such groups to perform critical operational functions at a lower cost, on a greater scale, or from distributed locations.
- Second, **extremists largely use the same platforms for the same purposes as an average internet user**. Like most people, adherents to extremist ideologies or organizations use the internet to communicate, socialize, buy and sell goods, and access information and entertainment. As detailed in other RAND work, much of this activity also occurs on mainstream platforms that host nonextremist content and might even maintain community terms of use that prohibit or restrict the sharing of extremist material.[53] Although specialist communities exist online, the notion of a separate extremist internet is a myth.

- Third, **extremists will likely adapt how they use the internet as new technologies become available and in response to counterextremism efforts**. Extremist groups across the ideological spectrum have shown themselves to be innovative and early users of new or unpopular technologies. They recognize the value of the online space, especially its ability to surmount geographic barriers and individual inhibitions. We should expect that extremists will not concede the online space easily. We have already seen how "alt-tech" platforms allow extremists to circumvent deplatforming. Countering extremists' use of the internet, therefore, will involve persistent and coordinated efforts to monitor and anticipate changes in virtual tactics and strategies.

But for all the power of the internet, even movements that have invested heavily in building a virtual presence continue to see in-person demonstrations as necessary to convey strength, attract a substantial number of members, and ultimately influence political institutions and policy decisions.[54] For extremist groups that advocate the use of violence, online organizing is no substitute for the psychological and material effects of real-world violence. Accordingly, the following section discusses what researchers have learned about how virtual interactions can encourage adoption of extremist ideologies and incite or inspire individuals to act offline.

WHAT IS RADICALIZATION?

We define *radicalization* as the psychological and behavioral process by which an individual is immersed in, and ultimately adopts, an extremist ideology.

HOW INTERNET USERS ENGAGE WITH EXTREMISM ONLINE

In recent years, researchers have rededicated their attention to a second, related line of inquiry: How does the availability of online extremist content influence offline behavior? This research comes amid efforts by policymakers, researchers, and civil society actors to understand whether and how society's growing reliance on the internet has altered communal political and social dynamics. High-profile examples of virtual encounters inspiring offline acts of violence, as well as growing evidence of the negative psychological effects of excessive internet use, have prompted questions about the harmful social and political effects of the growth in internet usage. The resulting literature has demonstrated that social media, internet-based communication technologies, and other digital platforms play an important role in encouraging political polarization, aiding the spread of false or misleading information, and amplifying conspiracy theories.[55] Of particular interest for this Perspective, such research has also suggested that exposure to extremist communities and content online may encourage the adoption of radical norms, ideas, and behavior and ultimately influence individual users' propensity for violence.[56]

That virtual interactions can inspire or encourage adoption of radical beliefs is well documented in court records, interviews, surveys of current and former extremists, and other empirical analyses of individual pathways to radicalization.[57] Although the international community has prioritized countering online recruitment to Islamist extremism until very recently,[58] this phenomenon has been documented in movements across the ideological spectrum.[59] For instance,

one study based on in-depth interviews with ten former members of violent far-right groups found that "participants overwhelmingly suggested that the Internet played an important role in facilitating their process of radicalization to violence, largely because it provided them with unfettered access to extreme right-wing content and a network of like-minded individuals, which in turn increased their exposure to violent extremist ideologies and violent extremist groups."[60]

Several unique characteristics of the internet make it an effective medium for individual radicalization. The first is the prevalence of virtual *echo chambers* that immerse users in homogeneous media environments. Online, the natural human tendency to socialize with like-minded individuals and to seek out information that affirms prior beliefs is reinforced through algorithmic systems that are designed to anticipate user desires and to customize the presentation of information according to demonstrated preferences.[61]

SOCIAL MEDIA: HOMOGENEOUS BY DESIGN?

Some researchers have raised concerns over the echo chamber metaphor, arguing that it oversimplifies the relationship between social media and other information sources. However, they also find that individuals with extreme views are more likely to drift into homogeneous social spaces (Geiß et al., 2021).

This effect appears to be particularly pronounced in virtual discussions of political issues. For example, a 2015 analysis of 3.8 million Twitter users observed that political discussions on the platform were characterized by higher degrees of ideological segregation and selective exposure compared with discussions of nonpolitical issues. Moreover, public conversations about national topics, such as the 2012 Newtown, Connecticut school shooting, transformed "fairly rapidly into highly polarized exchanges" with an attending decrease in cross-partisan exchange.[62] Over time, this trend toward insularity has produced ideological segregation within specific platforms and high levels of polarization among internet communities.

For some internet users, consistent exposure to like-minded virtual communities can discourage consideration of differing views and foster adoption of more-extreme norms and practices.[63] Through both passive interactions, such as the absorption of material selected and presented for consumption through algorithmic selections, and active decisions, such as the use of search functions to find extremist content or virtual communities, users can become cloistered within radical-information environments to a degree that is difficult to replicate in the physical world.[64] Indeed, the potential homogeneity of virtual environments is one of the factors that makes online recruitment strategies attractive to recruiters and propagandists. Through social media platforms, discussion forums, and other websites, charismatic influencers can isolate susceptible users from contrary messages and ensure their consistent exposure to the desired narrative.[65] "As a result," one scholar of radicalization has observed, "people acquire a skewed sense of reality so that extremist attitudes and violence are no longer taboos but—rather—are seen as positive and desirable."[66]

The anonymity and artificiality of virtual interactions may also lower inhibitions and suppress perceptions of differences among users, increasing trust in others' description of reality

and fostering group identification—dynamics that, in turn, increase users' susceptibility to more-extreme positions.[67] As alignment with an in-group increases, tolerance for differing opinions—and the groups that hold them—decreases, creating a self-reinforcing cycle of commitment to the in-group's norms and isolation from or rejection of differing viewpoints.[68] One study of Twitter users, for instance, found that those who held more-extreme views were less likely to engage in ideologically diverse interactions online.[69] In extreme cases, virtual social networks may shield radicalizing or radicalized individuals from contrary descriptions of reality, inhibiting adoption of more-moderate positions and fortifying their extremist views. In such cases, this rigidity can manifest as anger, hatred, and a desire to act against the perceived threat posed by outsiders.[70]

This process of *other deindividuation*, or the categorization of the world into in- and out-groups, can increase negative attitudes and even encourage aggression toward members of the perceived out-group.[71] As one study of radicalization to far-right movements suggested, the perceived privacy of internet forums, combined with the decreased danger of experiencing any social resistance or backlash, may encourage individuals both to use more-aggressive language and to issue direct calls for action.[72] Likening the activity of trading insults online to engaging in physical altercations, RAND's previous work on extremists' pathways to radicalization concluded that aggressive virtual behavior has "addictive properties [that] appear linked to the experience of joint risk and struggle and likely involve core psychological rewards linked with thrill-seeking, righteous anger, and in-group belonging."[73] Engagement in radical discourse on social media and discussion forums may therefore reinforce identification with extremist groups, encourage adoption of radical norms, and contribute to ideological hardening. A recent quantitative study found that participation in *subversive online activity* (defined by the authors as behaviors meant to abuse and harass others and engagement with niche subcultural platforms on which this behavior occurs) increased an individual's susceptibility to far-right extremist propaganda.[74]

Moreover, the mechanics of social media platforms may foster a sense of group identification by normalizing previously taboo views and reinforcing adherence to group values, norms, and attitudes. Perhaps the most notable examples are YouTube's content-recommendation system, which has been criticized widely for privileging divisive or incendiary content and entrapping viewers in a "hate-inducing" spiral of increasingly one-sided and extreme content, and Facebook's reaction algorithm, which encouraged the spread of misinformation and malicious content by boosting the dissemination of content that angered viewers.[75]

THE TUG OF MORE-EXTREME CONTENT

A contemporaneous study based on a large-scale audit of 30,925 videos posted on 349 channels (and the approximately 72 million associated comments) found evidence that "users consistently migrate from milder to more extreme content" (Ribeiro et al., 2020, p. 131).

Similarly, an analysis of content shared on a controversial subreddit (a user-created community on the discussion website Reddit) found that the website's upvoting and downvoting features minimized subscribers' exposure to contrary content

and provided incentives for members to either adopt or mimic the community's rhetorical and ideological preferences. As the authors concluded, the upvoting feature therefore "functioned to promote and normalize otherwise unacceptable views . . . to produce a one-sided narrative that serves to reinforce members' extremist views, thereby strengthening bonds between members of the in-group."[76]

In addition to facilitating indoctrination and increasing the number of people exposed to radical ideas, the online environment may accelerate radicalization on an individual- and community-level basis. Analysis of data collected on the social media activities of 479 extremists who radicalized between 2005 and 2016, for instance, found that the average amount of time between first exposure to extremist beliefs and first participation in extremist acts shrunk over time while the average rate of social media use grew.[77] Using an epidemiological approach, one study equated exposure to radical ideas online to exposure to a complex contagion, finding that such ideas spread through a social media community much like an infection spreads through a physical population. Noting that offline and online activity could not be easily dissociated, the author concluded that social media usage "enhance[d] the spread of extremist ideology" by providing the "reinforcement . . . required for transmission."[78]

However, scholars continue to disagree over whether the availability (and growing quantity) of incendiary content online has contributed to an overall increase in the number of violent actors or violent incidents. Several studies have noted an association in the timing, frequency, or location of online and offline hate incidents that suggests that virtual encounters can incite, encourage, or direct physical harms.[79] These findings align with suggestive evidence that increased participation in virtual extremist communities corresponds with changes in offline behavior.[80] Several studies of political civic engagement have indicated that participation in online political groups correlates with offline political activism, although these were not specific to the use of violence by individuals enculturated into an extremist belief system.[81]

Others have suggested that consumption of virtual propaganda may encourage adherents of extremist groups to translate grievances into violent action.[82] For instance, a study evaluating the effects of exposure to violent content on social media found a strong association with participation in offline political violence, with the strongest effects recorded among individuals who sought out extremist content rather than consuming it passively or accidentally.[83] "[S]ignalling allegiance to a group or ideology often becomes an all-consuming project for extremists . . . [who] need to prove themselves as 'down for the cause' or 'white enough' by committing more and more time and energy," the study's authors explained. "This performance of dedication often escalates in a competitive fashion, resulting in hate speech and violence."[84]

Nonetheless, there is insufficient evidence to suggest that exposure to virtual extremist communities alone is enough to motivate someone to enact violence in the real world. For instance, one quantitative assessment of known violent offenders found "little evidence to suggest that the Internet was the sole explanation prompting actors to decide to engage in a violent act."[85] Rather, the authors noted that most of the perpetrators had held radical views before they engaged with virtual extremist communities and used the internet largely for instrumental purposes, such as to plan an operation, learn new tactics, or conduct surveillance of an identified target.[86] This aligns with earlier work theorizing that social media contributes to political violence by facilitating access to practical information (e.g., the location of potential targets, techniques

for manufacturing explosives) and providing the social reinforcement necessary to prepare potential perpetrators emotionally, but does not substantially alter an individual's propensity for violence.[87] To the contrary, as the internet has made it easier to find and interact with extremist communities, it may have also enabled susceptible people to express their support for a movement without incurring the social, legal, or bodily risk of acting on these views in the physical world.[88]

These scholarly disagreements about the internet's role in driving violent offline behavior reflect, in part, the broader debate over how to conceptualize the radicalization process and to explain the interaction between external environmental factors and individual characteristics in encouraging acts of violence.[89] Such uncertainties reflect our general lack of understanding about what motivates people to be violent. Nonetheless, three themes are apparent at this stage of the scholarship:

- The architecture of the internet is conducive for radicalizing users to adopt extremist ideas or behaviors, including incitement to violence.
- The internet provides potentially violent actors with new ways to acquire the training, knowledge, and motivation to conduct attacks without direct recruitment by formal extremist groups. This potential is underscored by so-called lone wolf attacks by perpetrators who engage with online extremist communities but operate independently.[90]
- The number of people exposed to radical ideas has risen with the growth of the number of internet users and the popularization of message forums, social media networks, and other virtual communities. In turn, the percentage of the population that subscribes to radical ideologies is expected to increase—and some subset of that population will go so far as to use violence to promote their ideas.

COUNTERING VIRTUAL EXTREMISM

The challenge of combating online extremist activity—and managing its offline consequences—likely will preoccupy international governments, community organizations, and major technology companies for years to come. Despite continued methodological and definitional differences, researchers agree that the internet plays an important role in enabling extremists to perform critical operational functions, to promote their ideas, and to encourage harmful online and offline behaviors.

Numerous governmental, educational, and civil sector entities seek to disrupt extremists' attempts to exploit the internet and to impede the indoctrination of individuals online. Such initiatives include using automated tools to remove or refute violent, hateful, or otherwise harmful content, in the hope that this will inhibit the spread of this material online.[91]

BUILDING THE RIGHT TOOLKIT

RAND researchers have designed a variety of tools to counter extreme and malign content online. See, for instance, recent reports on the potential use of Twitter to empower ISIS opponents (Helmus and Bodine-Baron, 2017), social media bots to deliver counter-radicalization content to targets of extremist recruitment efforts (Marcellino et al., 2020b), and machine learning tools to detect misinformation and conspiracy theories online (Marcellino et al., 2020a; Marcellino et al., 2021).

There are also efforts to deny extremists access to virtual platforms that can be used to generate revenue, amplify their messages, or coordinate their activities.[92] In addition, the U.S. government has endorsed proactive measures to promote individual and community resiliency and to improve internet users' ability to identify manipulative information.[93] Yet researchers have not yet reached consensus on the relative effectiveness of these various strategies, and a RAND analysis of proposed frameworks to evaluate counterextremism programming found that most had significant methodological shortfalls.[94]

Nonetheless, the literature suggests that disrupting extremists' use of the internet will require two types of action: content moderation and removal (commonly described as *deplatforming*) and tailored counternarrative and strategic communication campaigns to prevent radicalization, promote community resiliency, and aid the deradicalization and reintegration of extremist adherents. Studies analyzing the effects of mass content removals on extremist activity found that they reduced the size of the audience exposed to extremist messages, degraded the effectiveness of some extremist propaganda, and forced extremist groups to divert resources to rebuilding their networks.[95] One influential study of Reddit's 2015 decision to close subreddits that violated its terms of use found that this action contributed to an 80-percent decrease in hate speech usage across the *entire* platform.[96]

But technological solutions alone are imperfect because extremists can still disseminate their messages to smaller audiences on alternative platforms, where the conviction of remaining followers may harden, or alter their language to circumvent restrictions on major platforms.[97] Researchers have cautioned that the sheer number of far-right groups, their co-option of popular memes and internet jargon, and their tendency to avoid using the explicit branding seen in ISIS and other Islamist propaganda make them particularly resilient to content-filtering and content-removal programs.[98] Disagreements over how to define hate speech also present barriers to designing effective tools to detect and disrupt extremist behavior online.[99]

Moreover, researchers generally agree that addressing the underlying drivers of extremism requires effective counter-messaging and community programming.[100] To date, however, the majority of the research that evaluates the efficacy of prevention and deradicalization programs has focused on religiously motivated extremism, and more research is needed to assess their applicability to far-right and white-supremacist movements.[101]

Disagreements over who should produce and disseminate counternarratives also present an impediment to designing and implementing new programs.[102] Who should be responsible for producing counterextremism material: technology platforms, federal or local government entities, or public interest groups? These debates raise fundamental and divisive questions about the importance of free speech, the appropriate role of government regulation, and the balance between indi-

CONTENT MODERATION IS A GLOBAL CHALLENGE

Extremist and malicious actors may also exploit international variations in how companies design and implement their content-moderation measures. Internal Facebook documents published by the *New York Times*, for instance, suggest that the platform's less stringent policies in Ethiopia, Sri Lanka, India, and Malaysia enabled users in those countries to exploit the platform to issue mass, coordinated calls for violence.

vidual rights and community welfare. While some have called for the federal government to regulate online content or to compel technology companies to strengthen their moderation policies, others have argued that stricter action would amount to an undue restriction or burden on constitutionally protected activities.[103] Likewise, policymakers, technology companies, and activists have struggled to reconcile the need to minimize the social harms associated with extremism, on the one hand, with the principles of a free and open internet on the other.[104] Any effort to disrupt extremists' use of the internet requires consideration of these trade-offs, as well as attention to who is responsible for executing these initiatives, which techniques offer the most-promising outcomes, and what should receive scarce resources.

SUGGESTIONS FOR FUTURE RESEARCH

Regardless of which strategy or strategies the various stakeholders choose to prioritize, the success of future counter-extremism initiatives will require continued efforts to deepen our understanding of how extremist groups employ technology; how virtual interactions both mimic and differ from in-person interactions; and how the producers, consumers, and disseminators of extremist content behave online. Our review identified six commonly noted information gaps or areas for additional study:

- ethnographic and descriptive analyses of non-Jihadist and non-Islamist extremist movements, including global far-right and violent misogynist movements
- comparative research among groups, countries, digital platforms, and language communities
- more-robust analysis of whether and how demographic characteristics, such as age, gender, and education, serve as mediating factors in virtual engagement with extremist content and susceptibility to online radicalization[105]
- virtual ethnography, large-N analysis, and other qualitative and quantitative approaches that would make for a more-robust empirical foundation for research
- interdisciplinary research, including scholars working outside the field of terrorism studies
- descriptive research on the role of the internet and virtual platforms in contemporary extremist and terrorist movements.[106]

These suggestions would improve the quality of research in the field and fill outstanding gaps in knowledge. Building upon these recommendations, we propose four additional ways that researchers could aid policymakers, law enforcement agencies, and other practitioners in developing new tools to address the challenge of online extremism:

- **Evaluate the relative effectiveness of virtual propaganda, recruitment, and radicalization efforts.** Existing research describes how online tools can disseminate radical messages but has not sufficiently explained whether virtual propaganda or recruiter interactions are more or less persuasive than similar offline tactics are. Does an individual who engages with extremism online demonstrate the same level of commitment to the ideological cause as an adherent who radicalized principally offline? Could there be a greater opportunity for virtual participants to disengage from the movement? Do the same messages resonate online as they do offline—and, if not, should counter-radicalization initiatives promote different messages in different domains? Has the internet enabled radical

movements to attract new types of adherents or simply improved their ability to reach a greater number of individuals? Are face-to-face and virtual interactions equally effective in inciting violent action?

- **Improve our understanding of the early stages of radicalization of online extremists.** Analysts have proposed multiple frameworks to conceptualize radicalization and to explain why only some individuals adopt extremist views and behaviors.[107] However, less attention has been paid to how internet users progress along the interim stages of this process. How does an individual transition from being exposed to extremist material online to being indoctrinated to those beliefs and to acting on them offline? What percentage of internet users engage with extremist communities online but never participate in offline activities and interactions? What factors motivate or constrain this decisionmaking process? What explains the variation in the speed at which individuals radicalize? Improved understanding of the hurdles to completing the radicalization process could improve community monitoring and enable earlier interventions that limit individual or community harms.
- **Balance our understanding of online extremism across ideologies.**[108] Past research has described how the degree to which and the way in which extremists interact online may vary according to group organization, ideology, location, and other factors.[109] Analysts' focus over the past two decades on Islamic extremism has left gaps in our understanding of white supremacists, violent misogynists, and other violent extremists.[110] Additional research is required to develop a comprehensive explanation for why various groups pursue varied internet strategies. Greater insight into the strategic, cultural, technical, and even ideological factors informing this calculus could contribute to more-tailored interventions, improve threat monitoring, and anticipate the evolution of would-be extremist movements.
- **Examine the extent to which extremists are early adopters of technology.** The growing popularity and availability of low-cost encrypted communication tools have raised concerns that extremists may evade monitoring by "going dark," leading to a call for increased regulation of commercial applications such as WhatsApp, Telegram, and Signal.[111] A growing body of analysis has demonstrated that extremist groups and movements use such platforms and that some extremists have even adapted related source code to develop their own tailored tools.[112] But less is known about whether and how extremists' use of encrypted platforms fundamentally differs from their activity on public and nonencrypted platforms. Improved understanding of this phenomenon is necessary to help policymakers, the private sector, and other stakeholders refine their strategies to counter radicalization and adapt to the changing technology landscape.

NOTES

[1] Christchurch Call, "The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online," undated. The announcement coincided with the two-year anniversary of the first Christchurch Call to Action Summit, which was hosted in Paris on May 7, 2019.

[2] White House, "Statement by Press Secretary Jen Psaki on the Occasion of the United States Joining the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online," press statement, May 7, 2021.

[3] Executive Office of the President, *National Strategy for Countering Domestic Terrorism*, Washington, D.C.: National Security Council and White House, June 2021, pp. 20–22; Zachary Cohen and Katie Bo Williams, "Biden Team May Partner with Private Firms to Monitor Extremist Chatter Online," CNN, May 3, 2021; Nomaan Merchant, "US to Ramp Up Tracking of Domestic Extremism on Social Media," Associated Press, May 20, 2021.

[4] For a brief description of online extremist activity over the 1980s and 1990s, see Maura Conway, Ryan Scrivens, and Logan Macnair, *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends*, The Hague: International Centre for Counter-Terrorism, October 2019, pp. 3–4; Joseph A. Schafer, "Spinning the Web of Hate: Web-Based Hate Propagation by Extremist Organizations," *Journal of Criminal Justice and Popular Culture*, Vol. 9, No. 2, 2002, pp. 69–70.

[5] Heather J. Williams, Alexandra T. Evans, Jamie Ryan, Erik E. Mueller, and Bryce Downing, *The Online Extremist Ecosystem: Its Evolution and a Framework for Separating Extreme from Mainstream*, Santa Monica, Calif.: RAND Corporation, PE-A1458-1, 2021. For a discussion of the role of social media in promoting conspiracy theories, see William Marcellino, Todd C. Helmus, Joshua Kerrigan, Hilary Reininger, Rouslan I. Karimov, and Rebecca Ann Lawrence, *Detecting Conspiracy Theories on Social Media: Improving Machine Learning to Detect and Understand Online Conspiracy Theories*, Santa Monica, Calif.: RAND Corporation, RR-A676-1, 2021.

[6] Stephane J. Baele, Lewys Brace, and Travis G. Coan coined the use of the term *ecosystem* to describe virtual networks of far-right activity in "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism*, ahead-of-print version, December 30, 2020, pp. 1–21.

[7] Alex Schmid, "Violent and Non-Violent Extremism: Two Sides of the Same Coin?" The Hague: International Centre for Counter-Terrorism, May 2014. For a discussion of the conceptual challenges and complications associated with the field's adoption of the term *extremism*, see Anthony Richards, "From Terrorism to 'Radicalization' to 'Extremism': Counterterrorism Imperative or Loss of Focus?" *International Affairs*, Vol. 91, No. 2, March 2015.

[8] In December 2021, the Department of Defense revised its regulations governing the handling of protest, extremist, and criminal gang activities by members of the armed forces to clarify the definition of "active participation in extremist activities," a category of prohibited behaviors. Per the regulation, *extremist activities* means advocating, engaging in, or supporting terrorism; the overthrow of the U.S. government or any political subdivision by force, violence, or other unconstitutional or unlawful means; the use of unlawful force, unlawful violence, or other illegal means to deprive individuals of their rights under federal, state, and local laws or to achieve goals that are political, religious, discriminatory, or ideological in nature; or violation of the laws of the U.S. government or any political subdivision. Membership in an extremist organization is not explicitly prohibited. Notably, the glossary included in the regulation does not include an entry for extremism (Department of Defense Instruction 1325.06, *Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces*, November 27, 2009, incorporating change 2, December 20, 2021, pp. 9–10).

[9] See Office of the Director of National Intelligence, "Domestic Violent Extremism Poses Heightened Threat in 2021," unclassified summary, Washington, D.C., March 1, 2021, p. 4.

[10] A good example of this is the U.S. government's introduction of the term *racially and ethnically motivated violent extremism*, acronymized as REMVE or RMVE, in late 2019. The intelligence community defines this term as domestic violent extremists "with ideological agendas derived from bias, often related to race or ethnicity, held by the actor against others, including a given population group" (Office of the Director of National Intelligence, 2021, p. 4). Read literally, this definition would include nearly any racial, ethnic, or caste-based violence worldwide. In practice, however, the term is used principally to describe white-oriented extremism, be it supremacy, separatism, or nationalism, in the United States and Europe and is not used to reference ideological violence within Africa, Asia, Latin America, or the Middle East. In contrast, the United Nations Counter-Terrorism Committee Executive Directorate uses *extreme right-wing terrorism* (ERWT), and the international Financial Action Task Force uses *ethnically or racially motivated terrorism* (EoRMT) interchangeably with ERWT. See United Nations Security Council, Counter-Terrorism Committee, Executive Directorate, "CTED Launches Trends Alert on 'Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism,'" press release, New York, April 1, 2020; Financial Action Task Force, *Ethnically or Racially Motivated Terrorism Financing*, Paris, France, June 2021.

[11] For example, the *National Strategy for Countering Domestic Terrorism*, released in June 2021, uses the same categories of domestic extremists used in the intelligence community's March 2021 assessment of domestic violent extremism (Executive Office of the President, 2021; Office of the Director of National Intelligence, 2021).

[12] Leadership Conference on Civil and Human Rights, "Leading Civil Rights Organizations Oppose Creation of New Domestic Terrorism Legislation," press release, Washington, D.C., January 19, 2021; Noa Yachot, "Fears Grow That Efforts to Combat US Domestic Terrorism Can Hurt Minorities," *The Guardian*, January 26, 2021; Patrick G. Eddington, "Biden's Domestic Terrorism Strategy: A Recipe for Civil Liberties Abuses?" *CATO at Liberty*, June 15, 2021; Ellen M. Gilmer, "Civil Liberties Worries Loom in Plan to Identify Insider Threats," *Bloomberg*, June 23, 2021; Betsy Woodruff Swan, "Biden's Domestic Terrorism Strategy Concerns Advocates," *Politico*, July 22, 2021. For a similar debate in the British context, see Recep Onursal and Daniel Kirkpatrick, "Is Extremism the 'New' Terrorism? The Convergence of 'Extremism' and 'Terrorism' in British Parliamentary Discourse," *Terrorism and Political Violence*, Vol. 33, No. 5, 2021.

[13] Aurelien Mondon and Aaron Winter, "Racist Movements, the Far Right and Mainstreaming," in John Solomos, ed., *Routledge International Handbook of Contemporary Racisms*, Abingdon, United Kingdom: Routledge, 2020. Since the 1980s, prominent U.S. white nationalists have sought to recast the movement, shifting attention from violent tactics to more generally acceptable notions of racial resentment and segregation in order to broaden their appeal, normalize and disseminate their ideas, and penetrate the national discourse (Stephanie L. Hartzell, "Alt-White: Conceptualizing the 'Alt-Right' as a Rhetorical Bridge Between White Nationalism and Mainstream Public Discourse," *Journal of Contemporary Rhetoric*, Vol. 8, No. 1/2, 2018; Anti-Defamation League, "Alt Right: A Primer on the New White Supremacy," webpage, undated). Despite this rhetorical tactic, similar levels of overt bias are found among those who identify overtly with extremist movements and those who use alternative terminology. See, for instance, Patrick S. Forscher and Nour S. Kteily, "A Psychological Profile of the Alt-Right," *Perspectives on Psychological Science*, Vol. 15, No. 1, January 2020.

[14] For a discussion of various conceptual approaches to the role of violence in extremism, see Schmid, 2014; Astrid Bötticher, "Towards Academic Consensus Definitions of Radicalism and Extremism," *Perspectives on Terrorism*, Vol. 11, No. 4, August 2017, pp. 73–74; and Jacob Aasland Ravndal and Tore Bjørgo, "Investigating Terrorism from the Extreme Right: A Review of Past and Present Research," *Perspectives on Terrorism*, Vol. 12, No. 6, December 2018, pp. 6–7. For an example of a definition of extremism as a criminal act, see Michael H. Becker, "When Extremists Become Violent: Examining the Association Between Social Control, Social Learning, and Engagement in Violent Extremism," *Studies in Conflict & Terrorism*, June 11, 2019, p. 2.

[15] For a discussion of the differences between extremism and terrorism, see Richards, 2015; Ravndal and Bjørgo, 2018, p. 7; Matthew M. Sweeney and Arie Perliger, "Explaining the Spontaneous Nature of Far-Right Violence in the United States," *Perspectives on Terrorism*, Vol. 12, No. 6, December 2018, p. 53; and Kathleen Deloughery, Ryan D. King, and Victor Asal, "Close Cousins or Distant Relatives? The Relationship Between Terrorism and Hate Crime," *Crime & Delinquency*, Vol. 58, No. 5, October 5, 2012. For a discussion of the definitional debate over the use of the term *terrorism*, see Leonard Weinberg, Ami Pedahzur, and Sivan Hirsch-Hoefler, "The Challenges of Conceptualizing Terrorism," *Terrorism and Political Violence*, Vol. 16, No. 4, 2004.

[16] We use Tinka Veldhuis and Jørgen Staun's distinction between *violent* extremism, which emphasizes the use of violence to achieve a goal, and a more-general conception of extremism as encompassing ideologies and movements that seek far-reaching changes in society but may or may not advocate the threat or use of violence. See Tinka Veldhuis and Jørgen Staun, *Islamist Radicalisation: A Root Cause Model*, The Hague: Netherlands Institute of International Relations Clingendael, October 2009, pp. 4–5.

[17] Because terrorism research generally reacts to rather than anticipates major events and trends, the field has been focused on religiously motivated jihadist groups since the September 11, 2001, attacks in the United States. Far-right terrorism and, by extension, far-right extremism have received comparatively less attention, even when measured in proportion to the number of such attacks in the United States and Europe (Bart Schuurman, "Topics in Terrorism Research: Reviewing Trends and Gaps, 2007–2016," *Critical Studies in Terrorism*, Vol. 12, No. 3, 2019). For a discussion of the tactical convergence between far-right and Islamist groups, see Daniel Köhler and Julia Ebner, "Strategies and Tactics: Communication Strategies of Jihadists and Right-Wing Extremists," in Johannes Baldauf, Julia Ebner, and Jakob Guhl, eds., *Hate Speech and Radicalisation Online: The OCCI Research Report*, London: Institute for Strategic Dialogue, 2019.

[18] See, for instance, Steven M. Furnell and Matthew J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers and Security*, Vol. 18, No. 1, 1999, pp. 30–32; Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Michael Jenkins, *Countering the New Terrorism*, Santa Monica, Calif.: RAND Corporation, MR-989-AF, 1999; Val Burris, Emery Smith, and Ann Strahm, "White Supremacist Networks on the Internet," *Sociological Focus*, Vol. 33, No. 2, 2000; Schafer, 2002; Brian Levin, "Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America," *American Behavioral Scientist*, Vol. 45, No. 6, February 2002; Fred Cohen, "Terrorism and Cyberspace," *Network Security*, Vol. 5, 2002; Phyllis B. Gerstenfeld, Diana R. Grant, and Chau-Pu Chiang, "Hate Online: A Content Analysis of Extremist Internet Sites," *Analyses of Social Issues and Public Policy*, Vol. 3, No. 1, 2003; Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Vol. 23, No. 1, Spring 2003; Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, Washington, D.C.: United States Institute of Peace, special report 116, March 2004; and Maura Conway, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security: An International Journal*, Vol. 19, 2006.

[19] This practice can be traced at least to the early 1990s, when websites soliciting donations to support the Taliban in Afghanistan and the mujahidin in Chechnya appeared (Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict & Terrorism*, Vol. 33, No. 4, 2010, p. 354).

[20] Weimann, 2004, pp. 7–8; Burris, Smith, and Strahm, 2000; Conway, 2006; Gerstenfeld, Grant, and Chiang, 2003; Yariv Tsfati and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict & Terrorism*, Vol. 25, No. 5, 2002.

[21] Jacobson, 2010, p. 357; W. Chris Hale, "Extremism on the World Wide Web: A Research Review," *Criminal Justice Studies*, Vol. 25, No. 4, 2012. Despite a growing effort by technology companies to implement new terms of service, analysis of prominent platforms, including PayPal, Squarespace, and Stripe, has found that white supremacists, anti-government militias, and other extremist groups have retained access to

these services (Institute for Strategic Dialogue and the Global Disinformation Index, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, London, October 27, 2020).

22 White supremacists, anti-immigration groups, and anti-government militias have organized campaigns on mainstream websites, such as Indiegogo and GoFundMe, although increased content moderation has contributed to a shift toward purpose-built platforms, such as GoyFundMe, Hatreon, and WeSearcher, that offer more-receptive environments (Anti-Defamation League, *Funding Hate: How White Supremacists Raise Their Money*, New York, 2017, pp. 10–12; Tom Keatinge, Florence Keen, and Kayla Izenman, "Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It," *RUSI Journal*, Vol. 164, No. 2, 2019, pp. 18–19).

23 Schafer, 2002, p. 79; Daniel Koehler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, No. 1, Winter 2014/2015.

24 Anti-Defamation League, 2017, p. 2.

25 Financial Action Task Force, 2021.

26 Jacobson, 2010.

27 Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America*, Cambridge, Mass.: Harvard University Press, 2018, pp. 120–121; Conway, Scrivens, and Macnair, 2019; Laura Smith, "Lone Wolves Connected Online: A History of Modern White Supremacy," *New York Times*, January 26, 2021; Chip Berlet, "When Hate Went Online," draft chapter, adapted from a paper presented at the Northeast Sociological Association, Spring Conference, Fairfield, Conn.: Sacred Heart University, April 28, 2001.

28 Conway, 2006, p. 16; Nico Prucha and Ali Fisher, "Tweeting for the Caliphate: Twitter as the New Frontier for Jihadi Propaganda," *CTC Sentinel*, Vol. 6, No. 6, June 2013, p. 21; Pete Simi, Steven Windisch, and Karyn Sporer, *Recruitment and Radicalization Among US Far-Right Terrorists*, College Park, Md.: National Consortium for the Study of Terrorism and Responses to Terrorism, November 2016, p. 91; Ryan Andrew Brown, Todd C. Helmus, Rajeev Ramchand, Alina I. Palimaru, Sarah Weilant, Ashley L. Rhoades, and Liisa Hiatt, *Violent Extremism in America: Interviews with Former Extremists and Their Families on Radicalization and Deradicalization*, Santa Monica, Calif.: RAND Corporation, RR-A1071-1, 2021, p. 89.

29 For a review of recent literature on online recruitment, see Ana-Maria Bliuc, Nicholas Faulkner, Andrew Jakubowicz, and Craig McGarty, "Online Networks of Racial Hate: A Systematic Review of 10 Years of Research on Cyber-Racism," *Computers in Human Behavior*, Vol. 87, October 2018, p. 82.

30 Koehler, 2014/2015.

31 J. M. Berger, "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *CTC Sentinel*, Vol. 8, No. 10, October 2015, p. 19. Another study based on interviews with young French jihadists who fought in Syria similarly found that consumption of online material played a critical role in their decisions to travel to fight (Hélène Bazex and Jean-Yves Mensat, "Qui sont les djihadistes Français? Analyse de 12 cas pour contribuer à l'évaluation du risqué de passage à l'acte [Who Are the French Jihadists? Analysis of 12 Cases to Help Develop Profiles and Assessment of the Risk of Acting Out]," *Annales Médico-Psychologiques,* Vol. 174, No. 4, 2016.

32 Koehler, 2014/2015, p. 118; Mason Youngblood, "Extremist Ideology as a Complex Contagion: The Spread of Far-Right Radicalization in the United States Between 2005 and 2017," *Humanities and Social Sciences Communications*, Vol. 7, No. 49, July 31, 2020, p. 7; European Union Agency for Law Enforcement Cooperation, *European Union Terrorism Situation and Trend Report 2020*, The Hague, 2020, pp. 72–73.

33 Thomas J. Holt, Joshua D. Freilich, and Steven M. Chermak, "Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures," *Deviant Behavior*, Vol. 38, No. 8, 2017, p. 864.

34 Tiana Gaudette, Ryan Scrivens, and Vivek Venkatesh, "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists," *Terrorism and Political Violence*, July 16, 2020, pp. 9–10.

[35] Gaudette, Scrivens, and Venkatesh, 2020, p. 10. For a similar finding, see Koehler, 2014/2015, p. 118.

[36] Pete Simi and Robert Futrell, "Cyberculture and the Endurance of White Power Activism," *Journal of Political and Military Sociology*, Vol. 34, No. 1, Summer 2006; Pete Simi and Robert Futrell, *American Swastika: Inside the White Power Movement's Hidden Spaces of Hate*, Lanham, Md.: Rowman & Littlefield, 2010; Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan, "Terrorist Use of the Internet by the Numbers," *Criminology & Public Policy*, Vol. 16, No. 1, February 2017; Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, Santa Monica, Calif., and Cambridge, United Kingdom: RAND Corporation, 2013.

[37] Conway, 2006, p. 11; John Curtis Amble, "Combating Terrorism in the New Media Environment," *Studies in Conflict & Terrorism*, Vol. 35, No. 5, 2012, p. 343.

[38] Charlie Winter, *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*, London: Qulliam, 2015; Moustafa Ayad, Amarnath Amarasingam, and Audrey Alexander, *The Cloud Caliphate: Archiving the Islamic State in Real-Time*, West Point, N.Y.: Combating Terrorism Center at West Point and the Institute for Strategic Dialogue, May 2021.

[39] Amble, 2012, p. 343.

[40] For instance, one study of ISIS-inspired violence in Europe found that 19 out of 38 plots planned during the period of study were informed by online instruction (Petter Nesser, Anne Stenersen, and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect," *Perspectives on Terrorism*, Vol. 10, No. 6, December 2016.

[41] Hale, 2012, p. 347.

[42] Julia Ebner, "Counter-Creativity: Innovative Ways to Counter Far-Right Communication Tactics," in Maik Fielitz and Nick Thurston, eds., *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*, Bielefeld, Germany: transcript Verlag, 2019a, pp. 171–172; Hale, 2012, p. 347; Bliuc et al., 2018, p. 82.

[43] Ahmad Shehabat and Teodor Mitew, "Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics," *Perspectives on Terrorism*, Vol. 12, No. 1, February 2018.

[44] In 2017, for instance, Stripe, PayPal, and Apple Pay joined domain service provider GoDaddy and website-hosting company Squarespace to deny services to organizations and individuals affiliated with the Unite the Right Rally (Katie Mettler and Avi Selk, "GoDaddy—then Google—Ban Neo-Nazi Site Daily Stormer for Disparaging Charlottesville Victim," *Washington Post*, August 14, 2017; Nick Statt, "Apple Pay Is Dropping Support for Websites That Sell White Supremacist Merchandise," *The Verge*, August 16, 2017; James Rufus Koren, "Can White Supremacist Groups Be Blocked from Raising Money Online? There's a Campaign to Try," *Los Angeles Times*, August 17, 2017; Tracy Jan, "PayPal Escalates the Tech Industry's War on White Supremacy," *Washington Post*, August 16, 2017).

[45] Adam Goldman and Eric Schmitt, "One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program," *New York Times*, November 24, 2016.

[46] For a discussion of the use of social media evidence in anti-terrorism legal proceedings, see Tasniem Anwar, "Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases," *International Political Sociology*, Vol. 14, No. 4, December 2020.

[47] Nellie Bowles, "How 'Doxxing' Became a Mainstream Tool in the Culture Wars," *New York Times*, August 30, 2017; David M. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology*, Vol. 18, No. 3, 2016.

[48] Olga Khazan, "The Far Right's Fear of 'Glowies,'" *The Atlantic*, January 25, 2021.

[49] Decca Muldowney, "Info Wars: Inside the Left's Online Efforts to Out White Supremacists," ProPublica, October 30, 2017;

Joey L. Blanch and Wesley L. Hsu, "An Introduction to Violent Crime on the Internet," *United States Attorneys' Bulletin*, Vol. 64, No. 3, May 2016. For a review of the literature on doxxing, see Briony Anderson and Mark A. Wood, "Doxxing: A Scoping Review and Typology," in Jane Bailey, Asher Flynn, and Nicola Henry, eds., *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Bingley, United Kingdom: Emerald Publishing Limited, 2021.

50 The emergence of a so-called alt-tech sector has received substantial media and academic attention. For discussions of this phenomenon and its consequences, see Julia Ebner, "Replatforming Unreality," *Journal of Design and Science*, September 5, 2019b; and Joan Donovan, Becca Lewis, and Brian Friedberg, "Parallel Ports: Sociotechnical Change from the Alt-Right to Alt-Tech," in Maik Fielitz and Nick Thurston, eds., *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*, Bielefeld, Germany: transcript Verlag, 2019. For a discussion of deplatforming's consequences for extremist user preferences, see Aleksandra Urman and Stefan Katz, "What They Do in the Shadows: Examining the Far-Right Networks on Telegram," *Information, Communication & Society*, 2020; Tamar Mitts, "Banned: How Deplatforming Extremists Mobilizes Hate in the Dark Corners of the Internet," conference paper, National Bureau of Economic Research Summer Institute, July 26, 2021; and Maura Conway, "Routing the Extreme Right: Challenges for Social Media Platforms," *RUSI Journal*, Vol. 165, No. 1, 2020.

51 Research by the Institute for Strategic Dialogue and the Global Disinformation Index similarly found that cryptocurrencies are the preferred funding mechanism for explicitly violent and decentralized organizations that have lost access to crowdfunding, onsite retail, and other mainstream virtual services (Institute for Strategic Dialogue and the Global Disinformation Index, 2020, p. 5). In August 2017, for instance, Matt Parrott of the Traditionalist Worker Party, a U.S.-based neo-Nazi group, announced a "sweeping shift" toward cryptocurrencies instead of the "traditional corporate internet" (Anti-Defamation League, 2017, p. 13). Affiliates of far-right forums, such as the Daily Stormer, Stormfront, Radio Aryan, and the National Policy Institute, reportedly have also begun to accept cryptocurrencies (Keatinge, Keen, and Izenman, 2019, p. 20). However, a RAND study of non-actor adoption suggests that technological barriers, uncertainty about the legitimacy of cryptocurrencies, and a general familiarity with traditional currencies could hinder more widespread adoption of cryptocurrencies (Joshua Baron, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, Santa Monica, Calif.: RAND Corporation, RR-1231-OSD, 2015).

52 See, for example, Christopher Ahlberg, "How Al-Qaeda Uses Encryption Post-Snowden (Part 2)—New Analysis in Collaboration with ReversingLabs," *Recorded Future*, August 1, 2014; Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel*, Vol. 9, No. 6, June 2016; Conway, Scrivens, and Macnair, 2019, pp. 14–16; Bennett Clifford and Helen Powell, *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram*, Washington, D.C.: Program on Extremism, George Washington University, June 2019; Jakob Guhl and Jacob Davey, *A Safe Space to Hate: White Supremacist Mobilisation on Telegram*, London: Institute for Strategic Dialogue, June 26, 2020; Richard Rogers, "Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media," *European Journal of Communication*, Vol. 35, No. 3, 2020; and Samantha Walther and Andrew McCoy, "US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism," *Perspectives on Terrorism*, Vol. 15, No. 2, April 2021. Researchers' emphasis on Telegram is a reflection of the fact that the application is relatively user-friendly and grants greater access to user data than other encrypted communication services. Other applications, such as Signal and WhatsApp, have received comparatively less attention from researchers.

53 Williams et al., 2021.

54 For an insightful analysis exploring this phenomenon in the context of the U.S. white-nationalist movement, see Donovan, Lewis, and Friedberg, 2019. This confirms earlier work based on interviews with German far-right extremists that suggested that such physical interactions as attending protests were

necessary for individuals to fully identify with a movement (Koehler, 2014/2015).

55 For a review of the literature on social media and political polarization, see Pablo Barberá, "Social Media, Echo Chambers, and Political Polarization," in Nathaniel Persily and Joshua A. Tucker, eds., *Social Media and Democracy: The State of the Field and Prospects for Reform*, Cambridge, United Kingdom: Cambridge University Press, 2020; and Christopher A. Bail, Lisa P. Argyle, Taylor W. Brown, John P. Bumpus, Haohan Chen, M. B. Fallin Hunzaker, Jaemin Lee, Marcus Mann, Friedolin Merhout, and Alexander Volfovsky, "Exposure to Opposing Views on Social Media Can Increase Political Polarization," *Proceedings of the National Academy of Sciences*, Vol. 115, No. 37, September 11, 2018. For a thoughtful review of the literature on the effect of the internet and social media on political outcomes, see Ekaterina Zhuravskaya, Maria Petrova, and Ruben Enikolopov, "Political Effects of the Internet and Social Media," *Annual Review of Economics*, Vol. 12, August 2020.

56 For examples of policy attention, see Quintan Wiktorowicz, "Working to Counter Online Radicalization to Violence in the United States," White House, archive, February 5, 2013; U.S. House of Representatives, Committee on Oversight and Government Reform, *Radicalization: Social Media and the Rise of Terrorism*, hearing before the Subcommittee on National Security, Washington, D.C., October 28, 2015; and United Nations Security Council Resolutions 2395 and 2396, both adopted on December 21, 2017.

57 For a debate over the utility of the concept and alternate definitions, see Mark Sedgwick, "The Concept of Radicalization as a Source of Confusion," *Terrorism and Political Violence*, Vol. 22, No. 4, 2010; Peter R. Neumann, "The Trouble with Radicalization," *International Affairs*, Vol. 89, No. 4, 2013; and Alexander Meleagrou-Hitchens and Nick Kaderbhai, *Research Perspectives on Online Radicalisation: A Literature Review, 2006–2016*, Dublin, Ireland: VOX-Pol Network of Excellence, 2017, pp. 13–17. For illustrative studies documenting the role of the internet in radicalization, see Von Behr et al., 2013; Mehmet F. Bastug, Aziz Douai, and Davut Akca, "Exploring the 'Demand Side' of Online Radicalization: Evidence from the Canadian Context," *Studies in Conflict & Terrorism*, Vol. 43, No. 7, 2020; and Brown et al., 2021.

58 See, for instance, Wiktorowicz, 2013; U.S. House of Representatives, Committee on Oversight and Government Reform, 2015; and United Nations Security Council Resolutions 2395 and 2396, both adopted December 21, 2017.

59 Von Behr et al., 2013; Koehler, 2014/2015; Brown et al., 2021.

60 Gaudette, Scrivens, and Venkatesh, 2020, p. 6.

61 Cass R. Sunstein popularized this concept with his book *Republic.com* (Princeton, N.J.: Princeton University Press, 2001) and with "The Law of Group Polarization," *Journal of Political Philosophy*, Vol. 10, No. 2, 2002. For examples of more-recent studies, see R. Kelly Garrett, "Echo Chambers Online? Politically Motivated Selective Exposure Among Internet News Users," *Journal of Computer-Mediated Communication*, Vol. 14, No. 2, 2009; Matthew J. Kushin and Kelin Kitchener, "Getting Political on Social Network Sites: Exploring Online Political Discourse on Facebook," *First Monday*, Vol. 14, No. 11, November 2009; Michael D. Conover, Jacob Ratkiewicz, Matthew Francisco, Bruno Gonçalves, Alessandro Flammini, and Fillipo Menczer, "Political Polarization on Twitter," *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*, Vol. 5, No. 1, 2021; Michael A. DeVito, "From Editors to Algorithms: A Values-Based Approach to Understanding Story Selection in the Facebook News Feed," *Digital Journalism*, Vol. 5, No. 6, 2017; Ivan Dylko, Igor Dolgov, William Hoffman, Nicholas Eckhart, Maria Molina, and Omar Aaziz, "Impact of Customizability Technology on Political Polarization," *Journal of Information Technology & Politics*, Vol. 15, No. 1, 2018; and James N. Cohen, "Exploring Echo-Systems: How Algorithms Shape Immersive Media Environments," *Journal of Media Literacy Education*, Vol. 10, No. 2, 2018. This human desire for opinion reinforcement and aversion to contrary information is well established. See, for instance, Peter H. Ditto and David F. Lopez, "Motivated Skepticism: Use of Differential Decision Criteria for Preferred and Nonpreferred Conclusions," *Journal*

of Personality and Social Psychology, Vol. 63, No. 4, 1992; and Miller McPherson, Lynn Smith-Lovin, and James M. Cook, "Birds of a Feather: Homophily in Social Networks," *Annual Review of Sociology*, Vol. 27, August 2001. In a shift from the early emphasis on algorithmic interference, researchers recently have begun to emphasize the interaction between passive environmental biases (e.g., how online platforms are designed to present users with homogeneous views) and user choices (e.g., to engage in secluded online spaces) (Eytan Bakshy, Solomon Messing, and Lada A. Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook," *Science*, Vol. 348, No. 6239, June 5, 2015; Daniele Valentini, Anna Maria Lorusso, and Achim Stephan, "*Onlife* Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization," *Frontiers in Psychology*, Vol. 11, March 2020).

62 Pablo Barberá, John T. Jost, Jonathan Nagler, Joshua A. Tucker, and Richard Bonneau, "Tweeting from Left to Right: Is Online Political Communication More Than an Echo Chamber?" *Psychological Science*, Vol. 26, No. 10, 2015, pp. 1539–1540.

63 Natalie Jomini Stroud, "Polarization and Partisan Selective Exposure," *Journal of Communication*, Vol. 60, No. 3, 2010; Magdalena Wojcieszak, "'Don't Talk to Me': Effects of Ideologically Homogeneous Online Groups and Politically Dissimilar Offline Ties on Extremism," *New Media & Society*, Vol. 12, No. 4, 2010. For a discussion of the importance of insularity for group identity formation in the real world, see Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, Philadelphia, Pa.: University of Pennsylvania Press, 2008. One study based on interviews with former white-supremacist skinheads described a process of exposure to radical content followed by a period of immersion within extremist communities online that granted a sense of community and encouraged adherence to increasingly extreme interpretations of their grievances (Gaudette, Scrivens, and Venkatesh, 2020, pp. 8–9). For a contrary view, see Jae Kook Lee, Jihyang Choi, Cheonsoo Kim, and Yonghwan Kim, "Social Media, Network Heterogeneity, and Opinion Polarization," *Journal of Communication*, Vol. 64, No. 4, August 2014.

64 Gaudette, Scrivens, and Venkatesh, 2020, p. 13; Conway, Scrivens, and Macnair, 2019.

65 Meleagrou-Hitchens and Kaderbhai, 2017, p. 7. For studies exploring the role of interactive sites in radicalizing individuals to accept militant Salafist ideologies, see Angela Gendron, "The Call to Jihad: Charismatic Preachers and the Internet," *Studies in Conflict & Terrorism*, Vol. 40, No. 1, 2017; and Berger, 2015. For studies exploring how the internet enables groups to control or influence the information presented to their members, see Joseph A. Carter, Shiraz Maher, and Peter R. Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, London: International Centre for the Study of Radicalisation and Political Violence, 2014; and Jytte Klausen, "Tweeting the *Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, Vol. 38, No. 1, 2015.

66 Peter Neumann, *Countering Online Radicalization in America*, Washington, D.C.: Bipartisan Policy Center, December 2012, p. 18.

67 The relationship between anonymity online and group identification is long recognized. For an early study describing this phenomenon during digital interaction, see Russell Spears, Martin Lea, and Stephen Lee, "De-Individuation and Group Polarization in Computer-Mediated Communication," *British Journal of Social Psychology*, Vol. 29, No. 2, June 1990. See also Koehler, 2014/2015, p. 118; and John Suler, "The Online Disinhibition Effect," *International Journal of Applied Psychoanalytic Studies,* Vol. 2, No. 2, June 2005.

68 R. Kelly Garrett, Brian E. Weeks, and Rachel L. Neo, "Driving a Wedge Between Evidence and Beliefs: How Online Ideological News Exposure Promotes Political Misperceptions," *Journal of Computer-Mediated Communication*, Vol. 21, No. 5, September 2016. This line of research builds upon psychological studies of intergroup dynamics. See, for instance, Diane M. Mackie, Thierry Devos, and Eliot R. Smith, "Intergroup Emotions: Explaining Offensive Action Tendencies in an Intergroup Context," *Journal of Personality and Social Psychology*, Vol. 79, No. 4, 2000.

[69] Andrei Boutyline and Robb Willer, "The Social Structure of Political Echo Chambers: Variation in Ideological Homophily in Online Networks," *Political Psychology*, Vol. 38, No. 3, June 2017.

[70] Mackie, Devos, and Smith, 2000; Jeremy A. Frimer, Mark J. Brandt, Zachary Melton, and Matt Motyl, "Extremists on the Left and Right Use Angry, Negative Language," *Personality and Social Psychology Bulletin*, Vol. 45, No. 8, 2019.

[71] For studies exploring this dynamic, see Blake M. Riek, Eric W. Mania, and Samuel L. Gaertner, "Intergroup Threat and Outgroup Attitudes: A Meta-Analytic Review," *Personality and Social Psychology Review*, Vol. 10, No. 4, 2006; Kurt Braddock, "The Utility of Narratives for Promoting Radicalization: The Case of the Animal Liberation Front," *Dynamics of Asymmetric Conflict*, Vol. 8, No. 1, 2015, p. 53; and John D. Gallacher, Marc W. Heerdink, and Miles Hewstone, "Online Engagement Between Opposing Political Protest Groups via Social Media Is Linked to Physical Violence of Offline Encounters," *Social Media + Society*, Vol. 7, No. 1, January–March 2021.

[72] Koehler, 2014/2015, p. 119.

[73] Brown et al., 2021, pp. xv, 87.

[74] Kurt Braddock, Brian Hughes, Beth Goldberg, and Cynthia Miller-Idriss, "Subversive Online Activity Predicts Susceptibility to Persuasion by Far-Right Extremist Propaganda," MediArXiv preprint article, 2021.

[75] For an example of the public scrutiny of YouTube's approach, see Kevin Roose, "The Making of a YouTube Radical," *New York Times*, June 8, 2019; and Cecilia D'Anastasio, "The Christchurch Shooter and YouTube's Radicalization Trap," *Wired*, December 8, 2020. For empirical studies of the recommendation algorithm's role in promoting extremist content and creating homogeneous media environments, see Luke Munn, "Angry by Design: Toxic Communication and Technical Architectures," *Humanities and Social Sciences Communications*, Vol. 7, No. 53, 2020, pp. 6–8; Daniel Röchert, Muriel Weitzel, and Björn Ross, "The Homogeneity of Right-Wing Populist and Radical Content in YouTube Recommendations," *Proceedings of the SMSociety '20: International Conference on Social Media and Society*, July 2020; Joe Whittaker, Seán Looney, Alastair Reed, and Fabio Votta, "Recommender Systems and the Amplification of Extremist Content," *Internet Policy Review*, Vol. 10, No. 2, 2021; and Annie Y. Chen, Brendan Nyhan, Jason Reifler, Ronald E. Robertson, and Christo Wilson, *Exposure to Alternative and Extremist Content on YouTube*, New York: Anti-Defamation League, undated. Mark Ledwich and Anna Zaitsev have refuted this assertion in a study of YouTube's content recommendation algorithm, which found that the system "fails to promote inflammatory or radicalized content, as previously claimed by several outlets" because there was insufficient evidence that an anonymous internet user would be directed toward more-extreme content" ("Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization," *First Monday*, Vol. 25, No. 3, March 2, 2020). However, the authors note that the study did not replicate the average internet user's experience over time and did not take into account how "the recommendation algorithm gets more fine-tuned and context-specific after each video that is watched." On Facebook's ranking algorithm, see Jeremy B. Merrill and Will Oremus, "Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation," *Washington Post*, October 26, 2021.

[76] Tiana Gaudette, Ryan Scrivens, Garth Davies, and Richard Frank, "Upvoting Extremism: Collective Identity Formation and the Extreme Right on Reddit," Global Network on Extremism & Technology, November 25, 2020.

[77] Brown et al., 2021, p. 19.

[78] Youngblood, 2020, p. 1.

[79] Ebner, 2019b; Matthew L. Williams, Pete Burnap, Amir Javed, Han Liu, and Sefa Ozalp, "Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime," *British Journal of Criminology*, Vol. 60, No. 1, January 2020; Karsten Müller and Carlo Schwarz, "Fanning the Flames of Hate: Social Media and Hate Crime," *Journal of the European Economic Association*, Vol. 19, No. 4, August 2021.

[80] For a review of the literature on internet subcultures that found similar correlations between online and offline behavior, see Holt, Freilich, and Chermak, 2017, pp. 860–861. For a study that found evidence that offline political engagement increases with greater participation in virtual extremist discussion forums, see Magdalena Wojcieszak, "'Carrying Online Participation Offline'—Mobilization by Radical Online Groups and Politically Dissimilar Offline Ties," *Journal of Communication*, Vol. 59, No. 3, 2009.

[81] Meredith Conroy, Jessica T. Feezell, and Mario Guerrero, "Facebook and Political Engagement: A Study of Online Political Group Membership and Offline Political Engagement," *Computers in Human Behavior*, Vol. 28, No. 5, September 2012; Lieven Pauwels and Nele Schils, "Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives," *Terrorism and Political Violence*, Vol. 28, No. 1, 2016; Bruce Hardy and Dietram A. Scheufele, "Examining Differential Gains from Internet Use: Comparing the Moderating Role of Talk and Online Interactions," *Journal of Communication*, Vol. 55, No. 1, March 2005; Kuang-Ting Tai, Gregory Porumbescu, and Jongmin Shon, "Can E-Participation Stimulate Offline Citizen Participation: An Empirical Test with Practical Implications," *Public Management Review*, Vol. 22, No. 2, 2020.

[82] Tom Holt, Joshua D. Freilich, Steven Chermak, and Clark McCauley, "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos," *Dynamics of Asymmetric Conflict*, Vol. 8, No. 2, 2015.

[83] Pauwels and Schils, 2016.

[84] Jigsaw, "Global, Connected and Decentralized," *The Current*, No. 2, 2020.

[85] Gill et al., 2017, p. 114.

[86] Gill et al., 2017, p. 114.

[87] Mattias Wahlström and Anton Törnberg, "Social Media Mechanisms for Right-Wing Political Violence in the 21st Century: Discursive Opportunities, Group Dynamics, and Co-Ordination," *Terrorism and Political Violence*, Vol. 33, No. 4, 2021.

[88] Manuel R. Torres-Soriano, "Barriers to Entry to Jihadist Activism on the Internet," *Studies in Conflict & Terrorism*, 2021. This work builds upon previous studies that look at the online behavior of members of other deviant subcultures. See, for instance, Kristie R. Blevins and Thomas J. Holt, "Examining the Virtual Subculture of Johns," *Journal of Contemporary Ethnography*, Vol. 38, No. 5, 2009.

[89] On this point, see Alexander Meleagrou-Hitchens, Audrey Alexander, and Nick Kaderbhai, "The Impact of Digital Communications Technology on Radicalization and Recruitment," *International Affairs*, Vol. 93, No. 5, September 2017, p. 1247.

[90] Gabriel Weimann, "Lone Wolves in Cyberspace," *Journal of Terrorism Research*, Vol. 3, No. 2, Autumn 2012; Paul Gill, John Horgan, and Paige Deckert, "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists," *Journal of Forensic Sciences*, Vol. 59, No. 2, March 2014; Jerrold M. Post, Cody McGinnis, and Kristen Moody, "The Changing Face of Terrorism in the 21st Century: The Communications Revolution and the Virtual Community of Hatred," *Behavioral Sciences and the Law*, Vol. 32, No. 3, May–June 2014, p. 323; Jerrold M. Post, "Terrorism and Right-Wing Extremism: The Changing Face of Terrorism and Political Violence in the 21st Century: The Virtual Community of Hatred," *International Journal of Group Psychotherapy*, Vol. 65, No. 2, 2015; Joel A. Capellan, "Lone Wolf Terrorist or Deranged Shooter? A Study of Ideological Active Shooter Events in the United States, 1970–2014," *Studies in Conflict & Terrorism*, Vol. 38, No. 6, 2015; Holt, Freilich, and Chermak, 2017; Jonathan Kenyon, Christopher Baker-Beall, and Jens Binder, "Lone-Actor Terrorism–A Systematic Literature Review," *Studies in Conflict & Terrorism*, March 4, 2021, pp. 12–13.

[91] For a single-volume overview of major counterextremism initiatives, see Spandana Singh, *Everything in Moderation: An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User-Generated Content*, Washington, D.C.:

New America, July 15, 2019. For RAND research, see Todd C. Helmus and Elizabeth Bodine-Baron, *Empowering ISIS Opponents on Twitter*, Santa Monica, Calif.: RAND Corporation, PE-227-RC, 2017; and William Marcellino, Madeline Magnuson, Anne Stickells, Benjamin Boudreaux, Todd C. Helmus, Edward Geist, and Zev Winkelman, *Counter-Radicalization Bot Research: Using Social Bots to Fight Violent Extremism*, Santa Monica, Calif.: RAND Corporation, RR-2705-DOS, 2020b.

92 For a discussion of the strengths and challenges of this approach, see Ethan Zuckerman and Chand Rajendra-Nicolucci, "Deplatforming Our Way to the Alt-Tech Ecosystem," Knight First Amendment Institute at Columbia University, January 11, 2021; Shiza Ali, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini, "Understanding the Effect of Deplatforming on Social Networks," *WebSci '21: 13th ACM Web Science Conference 2021*, June 2021; and Neil F. Johnson, Rhys Leahy, Nicholas Johnson Restrepo, Nicholas Velásquez, Minzhang Zheng, Pedro Manrique, Prajwal Devkota, and Stefan Wuchty, "Hidden Resilience and Adaptive Dynamics of the Global Online Hate Ecology," *Nature*, Vol. 573, 2019.

93 Executive Office of the President, 2021, p. 22. For examples of these measures, see Ashley L. Rhoades, Todd C. Helmus, James V. Marrone, Victoria Smith, and Elizabeth Bodine-Baron, *Promoting Peace as the Antidote to Violent Extremism: Evaluation of a Philippines-Based Tech Camp and Peace Promotion Fellowship*, Santa Monica, Calif.: RAND Corporation, RR-A233-3, 2020; and Alice Huguet, John F. Pane, Garrett Baker, Laura S. Hamilton, and Susannah Faxon-Mills, *Media Literacy Education to Counter Truth Decay: An Implementation and Evaluation Framework*, Santa Monica, Calif.: RAND Corporation, RR-A112-18, 2021.

94 Sina Beaghley, Todd C. Helmus, Miriam Matthews, Rajeev Ramchand, David Stebbins, Amanda Kadlec, and Michael A. Brown, *Development and Pilot Test of the RAND Program Evaluation Toolkit*, Santa Monica, Calif.: RAND Corporation, RR-1799-DHS, 2017, pp. 5–6; Jacopo Bellasio, Joanna Hofman, Antonia Ward, Fook Nederveen, Anna Knack, Arya Sofia Meranto, and Stijn Hoorens, *Counterterrorism Evaluation: Taking Stock and Looking Ahead*, Santa Monica, Calif., and Cambridge, United Kingdom: RAND Corporation, RR-2628-WODC, 2018, pp. 76–77. See also Amy-Jane Gielen, "Countering Violent Extremism: A Realist Review for Assessing What Works, for Whom, in What Circumstances, and How?" *Terrorism and Political Violence*, Vol. 31, No. 6, 2019, pp. 1149–1150.

95 Rogers, 2020, p. 215; J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Washington, D.C.: Brookings Institution, Analysis Paper No. 20, March 2015, p. 56; Lella Nuori, Nuria Lorenzo-Dus and Amy-Louise Watkin, "Following the Whack-a-Mole: Britain First's Visual Strategy from Facebook to Gab," London: Royal United Services Institute for Defence and Security Studies, Global Research Network on Terrorism and Technology Paper No. 4, July 4, 2019.

96 Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert, "You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech," *Proceedings of the ACM Human-Computer Interaction*, Vol. 1, No. CSCW, November 2017.

97 Rogers, 2020, p. 215; Paris Peace Forum, "Digital Platforms and Extremism: Are Content Controls Effective?" in *Insights from the 2018 Paris Peace Forum Debate Sessions*, November 13, 2018; Sheera Frenkel and Davey Alba, "In India, Facebook Grapples with an Amplified Version of Its Problems," *New York Times*, October 23, 2021.

98 Conway, 2020, pp. 108–110; Paris Peace Forum, 2018.

99 For illustrative studies on developing tools to detect hate speech, see Mainack Mondal, Leandro Araújo Silva, and Fabrício Benevenuto, "A Measurement Study of Hate Speech in Social Media," *HT '17: Proceedings of the 28th ACM Conference on Hypertext and Social Media*, July 2017; and Njagi Dennis Gitari, Zhang Zuping, Hanyurwimfura Damien, and Jun Long, "A Lexicon-Based Approach for Hate Speech Detection," *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 10, No. 4, 2015.

[100] Bharath Ganesh and Jonathan Bright, "Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation," *Policy & Internet*, Vol. 12, No. 1, March 2020, p. 8; Rachel Briggs and Sebastien Feve, *Review of Programs to Counter Narratives of Violent Extremism: What Works and What Are the Implications for Government?* London: Institute for Strategic Dialogue, 2013, p. 25.

[101] For helpful reviews of the literature on preventing extremism and countering extremist narratives, see Joshua Sinai with Jeffrey Fuller and Tiffany Seal, "Research Note: Effectiveness in Counter-Terrorism and Countering Violent Extremism: A Literature Review," *Perspectives on Terrorism*, Vol. 13, No. 6, December 2019; and William Stephens, Stijn Sieckelinck, and Hans Boutellier, "Preventing Violent Extremism: A Review of the Literature," *Studies in Conflict & Terrorism*, Vol. 44, No. 4, 2021. For an illustration of the emphasis on religious extremism to date, see the summary of evaluation studies in Beaghley et al., 2017, pp. 22–23.

[102] For a discussion of the "contested role between civil society, government, and the private sector," see Ganesh and Bright, 2020; and Anne Aly, Anne-Marie Balbi, and Carmen Jacques, "Rethinking Countering Violent Extremism: Implementing the Role of Civil Society," *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 10, No. 1, 2015.

[103] For a balanced discussion of the legal considerations when implementing counterextremist measures, see Victoria L. Killion, *Terrorism, Violent Extremism, and the Internet: Free Speech Considerations*, Washington, D.C.: Congressional Research Service, R45713, May 6, 2019. For an illustrative argument against government monitoring of social media on these grounds, see Rachel Levinson-Waldman and Sahil Singhvi, "Law Enforcement Social Media Monitoring Is Invasive and Opaque," Brennan Center for Justice, November 6, 2019.

[104] "Civil Society Positions on Christchurch Call Pledge," document prepared for the Civil Society leaders' Voices for Action meeting on May 14, 2019, with New Zealand Prime Minister Jacinda Ardern, 2019.

[105] For examples of work on this subject, see Angela Nienierza, Carsten Reinemann, Nayla Fawzi, Claudia Riesmeyer, and Katharina Neumann, "Too Dark to See? Explaining Adolescents' Contact with Online Extremism and Their Ability to Recognize It," *Information, Communication & Society*, Vol. 24, No. 9, 2021; Matthew Costello and James Hawdon, "Who Are the Online Extremists Among Us? Socio-Demographic Characteristics, Social Networking, and Online Experiences of Those Who Produce Online Hate Materials," *Violence and Gender*, Vol. 5, No. 1, March 2018; and Matthew Costello, James Hawdon, Thomas Ratliff, and Tyler Grantham, "Who Views Online Extremism? Individual Attributes Leading to Exposure," *Computers in Human Behavior*, Vol. 63, October 2016.

[106] This list is adapted from Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict & Terrorism*, Vol. 40, No. 1, Spring 2017; Peter Neumann and Scott Kleinmann, "How Rigorous Is Radicalization Research?" *Democracy and Security*, Vol. 9, No. 4, 2013; and Maura Conway and Stuart Macdonald, "Introduction to the Special Issue: Extremism and Terrorism Online—Widening the Research Base," *Studies in Conflict & Terrorism*, January 21, 2021.

[107] There is continued disagreement over how to conceptualize the radicalization process and its internal stages or milestones. Mitchell D. Silber and Arvin Bhatt's four-stage process, developed for the New York Police Department to explain radicalization, is widely used: (1) pre-radicalization, (2) self-identification, (3) indoctrination, and (4) "Jihadization" (Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York: New York City Police Department, 2007). Other influential conceptual approaches include those found in John Horgan, "From Profiles to *Pathways* and Roots to *Routes*: Perspectives from Psychology on Radicalization into Terrorism," *Annals of the American Academy of Political & Social Science*, Vol. 618, July 2008; and Clark McCauley and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," *Terrorism and Political Violence*, Vol. 20, No. 3, 2008. For helpful reviews of this literature, see

Michael King and Donald M. Taylor, "The Radicalization of Homegrown Jihadists: A Review of Theoretical Models and Social Psychological Evidence," *Terrorism and Political Violence*, Vol. 23, No. 4, 2011; Randy Borum, "Radicalization into Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security*, Vol. 4, No. 4, Winter 2011a; Randy Borum, "Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research," *Journal of Strategic Security*, Vol. 4, No. 4, Winter 2011b; and Matteo Vergani, Muhammad Iqbal, Ekin Ilbahar, and Greg Barton, "The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence About Radicalization into Violent Extremism," *Studies in Conflict & Terrorism*, Vol. 43, No. 10, 2020.

108 Conway, 2017; Schuurman, 2019, p. 476.

109 Torres-Soriano, 2021; Gill et al., 2017; Sara Doering, Garth Davies, and Raymond Corrado, "Reconceptualizing Ideology and Extremism: Toward an Empirically-Based Typology," *Studies on Conflict & Terrorism*, July 17, 2020.

110 Yasmine Ahmed and Orla Lynch, "Terrorism Studies and the Far Right—The State of Play," *Studies in Conflict & Terrorism*, August 11, 2021.

111 In July 2019, the home affairs ministers and attorneys general of the United States, Australia, Canada, New Zealand, and the United Kingdom issued a communiqué calling on technology companies to "include mechanisms in the design of their encrypted products and services whereby governments . . . can gain access to data in a readable and usable format" (Five Country Ministerial, "Joint Meeting of FCM and Quintet of Attorneys-General," London: Government of the United Kingdom, 2019). The following year, the governments of India and Japan joined the original parties in a statement reiterating the request for technology companies to build so-called backdoors into their encrypted platforms (U.S. Department of Justice, "International Statement: End-To-End Encryption and Public Safety," press release, Washington, D.C., October 11, 2020). For a discussion of the law enforcement challenges associated with extremists' use of encryption technologies, see James B. Comey and Sally Quillian Yates, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy," joint statement before the Senate Judiciary Committee, Washington, D.C., July 8, 2015; and Christopher Wray, "Worldwide Threats to the Homeland," statement before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., September 24, 2020.

112 For examples, see Office of the Director of National Intelligence, 2021, p. 2; Graham, 2016; and Guhl and Davey, 2020.

BIBLIOGRAPHY

Ahlberg, Christopher, "How Al-Qaeda Uses Encryption Post-Snowden (Part 2)—New Analysis in Collaboration with ReversingLabs," Recorded Future, August 1, 2014. As of September 3, 2021: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/

Ahmed, Yasmine, and Orla Lynch, "Terrorism Studies and the Far Right—The State of Play," *Studies in Conflict & Terrorism*, August 11, 2021.

Ali, Shiza, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini, "Understanding the Effect of Deplatforming on Social Networks," *WebSci '21: 13th ACM Web Science Conference 2021*, June 2021, pp. 187–195.

Aly, Anne, Anne-Marie Balbi, and Carmen Jacques, "Rethinking Countering Violent Extremism: Implementing the Role of Civil Society," *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 10, No. 1, 2015, pp. 3–13.

Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen, "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization," *Studies in Conflict & Terrorism*, Vol. 40, No. 1, 2017, pp. 1–9.

Amble, John Curtis, "Combating Terrorism in the New Media Environment," *Studies in Conflict & Terrorism*, Vol. 35, No. 5, 2012, pp. 339–353.

Anderson, Briony, and Mark A. Wood, "Doxxing: A Scoping Review and Typology," in Jane Bailey, Asher Flynn, and Nicola Henry, eds., *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Bingley, United Kingdom: Emerald Publishing Limited, 2021, pp. 205–226.

Anti-Defamation League, "Alt Right: A Primer on the New White Supremacy," webpage, undated. As of August 17, 2021: https://www.adl.org/resources/backgrounders/alt-right-a-primer-on-the-new-white-supremacy

Anti-Defamation League, *Funding Hate: How White Supremacists Raise Their Money*, New York, 2017.

Anwar, Tasniem, "Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases," *International Political Sociology*, Vol. 14, No. 4, December 2020, pp. 382–398.

Army Regulation 600-20, *Army Command Policy*, Washington, D.C.: Headquarters, Department of the Army, July 24, 2020.

Ayad, Moustafa, Amarnath Amarasingam, and Audrey Alexander, *The Cloud Caliphate: Archiving the Islamic State in Real-Time*, West Point, N.Y.: Combating Terrorism Center at West Point and the Institute for Strategic Dialogue, May 2021.

Baele, Stephane J., Lewys Brace, and Travis G. Coan, "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism*, ahead-of-print version, December 30, 2020, pp. 1–21.

Bail, Christopher A., Lisa P. Argyle, Taylor W. Brown, John P. Bumpus, Haohan Chen, M. B. Fallin Hunzaker, Jaemin Lee, Marcus Mann, Friedolin Merhout, and Alexander Volfovsky, "Exposure to Opposing Views on Social Media Can Increase Political Polarization," *Proceedings of the National Academy of Sciences*, Vol. 115, No. 37, September 11, 2018, pp. 9216–9221.

Bakshy, Eytan, Solomon Messing, and Lada A. Adamic, "Exposure to Ideologically Diverse News and Opinion on Facebook," *Science*, Vol. 348, No. 6239, June 5, 2015, pp. 1130–1132.

Barberá, Pablo, "Social Media, Echo Chambers, and Political Polarization," in Nathaniel Persily and Joshua A. Tucker, eds., *Social Media and Democracy: The State of the Field and Prospects for Reform*, Cambridge, United Kingdom: Cambridge University Press, 2020, pp. 34–55.

Barberá, Pablo, John T. Jost, Jonathan Nagler, Joshua A. Tucker, and Richard Bonneau, "Tweeting from Left to Right: Is Online Political Communication More Than an Echo Chamber?" *Psychological Science*, Vol. 26, No. 10, 2015, pp. 1539–1542.

Baron, Joshua, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, Santa Monica, Calif.: RAND Corporation, RR-1231-OSD, 2015. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RR1231.html

Bastug, Mehmet F., Aziz Douai, and Davut Akca, "Exploring the 'Demand Side' of Online Radicalization: Evidence from the Canadian Context," *Studies in Conflict & Terrorism*, Vol. 43, No. 7, 2020, pp. 616–637.

Bazex, Hélène, and Jean-Yves Mensat, "Qui sont les djihadistes Français? Analyse de 12 cas pour contribuer à l'évaluation du risqué de passage à l'acte [Who Are the French Jihadists? Analysis of 12 Cases to Help Develop Profiles and Assessment of the Risk of Acting Out]," *Annales Médico-Psychologiques*, Vol. 174, No. 4, 2016, pp. 257–265.

Beaghley, Sina, Todd C. Helmus, Miriam Matthews, Rajeev Ramchand, David Stebbins, Amanda Kadlec, and Michael A. Brown, *Development and Pilot Test of the RAND Program Evaluation Toolkit for Countering Violent Extremism*, Santa Monica, Calif.: RAND Corporation, RR-1799-DHS, 2017. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RR1799.html

Becker, Michael H., "When Extremists Become Violent: Examining the Association Between Social Control, Social Learning, and Engagement in Violent Extremism," *Studies in Conflict & Terrorism*, June 11, 2019.

Belew, Kathleen, *Bring the War Home: The White Power Movement and Paramilitary America*, Cambridge, Mass.: Harvard University Press, 2018.

Bellasio, Jacopo, Joanna Hofman, Antonia Ward, Fook Nederveen, Anna Knack, Arya Sofia Meranto, and Stijn Hoorens, *Counterterrorism Evaluation: Taking Stock and Looking Ahead*, Santa Monica, Calif., and Cambridge, United Kingdom: RAND Corporation, RR-2628-WODC, 2018. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RR2628.html

Berger, J. M., "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *CTC Sentinel*, Vol. 8, No. 10, October 2015, pp. 19–23.

Berger, J. M., and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Washington, D.C.: Brookings Institution, Analysis Paper No. 20, March 2015.

Berlet, Chip, "When Hate Went Online," draft chapter, adapted from a paper presented at the Northeast Sociological Association, Spring Conference, Fairfield, Conn.: Sacred Heart University, April 28, 2001.

Blanch, Joey L., and Wesley L. Hsu, "An Introduction to Violent Crime on the Internet," *United States Attorneys' Bulletin*, Vol. 64, No. 3, May 2016, pp. 2–12.

Blevins, Kristie R., and Thomas J. Holt, "Examining the Virtual Subculture of Johns," *Journal of Contemporary Ethnography*, Vol. 38, No. 5, 2009, pp. 619–648.

Bliuc, Ana-Maria, Nicholas Faulkner, Andrew Jakubowicz, and Craig McGarty, "Online Networks of Racial Hate: A Systematic Review of 10 Years of Research on Cyber-Racism," *Computers in Human Behavior*, Vol. 87, October 2018, pp. 75–86.

Bloom, Mia, Hicham Tiflati, and John Horgan, "Navigating ISIS's Preferred Platform: Telegram," *Terrorism and Political Violence*, Vol. 31, No. 6, 2019, pp. 1242–1254.

Borum, Randy, "Radicalization into Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security*, Vol. 4, No. 4, Winter 2011a, pp. 7–36.

Borum, Randy, "Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research," *Journal of Strategic Security*, Vol. 4, No. 4, Winter 2011b, pp. 37–62.

Bötticher, Astrid, "Towards Academic Consensus Definitions of Radicalism and Extremism," *Perspectives on Terrorism*, Vol. 11, No. 4, August 2017, pp. 73–77.

Boutyline, Andrei, and Robb Willer, "The Social Structure of Political Echo Chambers: Variation in Ideological Homophily in Online Networks," *Political Psychology*, Vol. 38, No. 3, June 2017, pp. 551–569.

Bowles, Nellie, "How 'Doxxing' Became a Mainstream Tool in the Culture Wars," *New York Times*, August 30, 2017.

Braddock, Kurt, "The Utility of Narratives for Promoting Radicalization: The Case of the Animal Liberation Front," *Dynamics of Asymmetric Conflict*, Vol. 8, No. 1, 2015, pp. 38–59.

Braddock, Kurt, Brian Hughes, Beth Goldberg, and Cynthia Miller-Idriss, "Subversive Online Activity Predicts Susceptibility to Persuasion by Far-Right Extremist Propaganda," MediArXiv preprint article, 2021. As of October 20, 2021: https://mediarxiv.org/c734s/

Briggs, Rachel, and Sebastien Feve, *Review of Programs to Counter Narratives of Violent Extremism: What Works and What Are the Implications for Government?* London: Institute for Strategic Dialogue, 2013.

Brown, Ryan Andrew, Todd C. Helmus, Rajeev Ramchand, Alina I. Palimaru, Sarah Weilant, Ashley L. Rhoades, and Liisa Hiatt, *Violent Extremism in America*: *Interviews with Former Extremists and Their Families on Radicalization and Deradicalization*, Santa Monica, Calif.: RAND Corporation, RR-A1071-1, 2021. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RRA1071-1.html

Burris, Val, Emery Smith, and Ann Strahm, "White Supremacist Networks on the Internet," *Sociological Focus*, Vol. 33, No. 2, 2000, pp. 215–235.

Capellan, Joel A., "Lone Wolf Terrorist or Deranged Shooter? A Study of Ideological Active Shooter Events in the United States, 1970–2014," *Studies in Conflict & Terrorism*, Vol. 38, No. 6, 2015, pp. 395–413.

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

Chandrasekharan, Eshwar, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert, "You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech," *Proceedings of the ACM Human-Computer Interaction*, Vol. 1, No. CSCW, November 2017, pp. 1–22.

Chen, Annie Y., Brendan Nyhan, Jason Reifler, Ronald E. Robertson, and Christo Wilson, *Exposure to Alternative and Extremist Content on YouTube*, New York: Anti-Defamation League, undated.

Chermak, Steven, Joshua Freilich, and Michael Suttmoeller, "The Organizational Dynamics of Far-Right Hate Groups in the United States: Comparing Violent to Nonviolent Organizations," *Studies in Conflict & Terrorism*, Vol. 36, No. 3, 2013, pp. 193–218.

Christchurch Call, "The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online," undated.

"Civil Society Positions on Christchurch Call Pledge," document prepared for the Civil Society leaders' Voices for Action meeting on May 14, 2019, with New Zealand Prime Minister Jacinda Ardern, 2019.

Clifford, Bennett, and Helen Powell, *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram*, Washington, D.C.: Program on Extremism, George Washington University, June 2019.

Cohen, Fred, "Terrorism and Cyberspace," *Network Security*, Vol. 5, 2002, pp. 17–19.

Cohen, James N., "Exploring Echo-Systems: How Algorithms Shape Immersive Media Environments," *Journal of Media Literacy Education*, Vol. 10, No. 2, 2018, pp. 139–151.

Cohen, Zachary, and Katie Bo Williams, "Biden Team May Partner with Private Firms to Monitor Extremist Chatter Online," CNN, May 3, 2021.

Comey, James B., and Sally Quillian Yates, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy," joint statement before the Senate Judiciary Committee, Washington, D.C., July 8, 2015.

Conover, Michael D., Jacob Ratkiewicz, Matthew Francisco, Bruno Gonçalves, Alessandro Flammini, and Fillipo Menczer, "Political Polarization on Twitter," *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*, Vol. 5, No. 1, 2021, pp. 89–96.

Conroy, Meredith, Jessica T. Feezell, and Mario Guerrero, "Facebook and Political Engagement: A Study of Online Political Group Membership and Offline Political Engagement," *Computers in Human Behavior*, Vol. 28, No. 5, September 2012, pp. 1535–1546.

Conway, Maura, "Terrorist 'Use' of the Internet and Fighting Back," *Information & Security: An International Journal*, Vol. 19, 2006, pp. 9–30.

Conway, Maura, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict & Terrorism*, Vol. 40, No. 1, Spring 2017, pp. 77–98.

Conway, Maura, "Routing the Extreme Right: Challenges for Social Media Platforms," *RUSI Journal*, Vol. 165, No. 1, 2020, pp. 108–113.

Conway, Maura, and Stuart Macdonald, "Introduction to the Special Issue: Extremism and Terrorism Online—Widening the Research Base," *Studies in Conflict & Terrorism*, January 21, 2021.

Conway, Maura, Ryan Scrivens, and Logan Macnair, *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends*, The Hague: International Centre for Counter-Terrorism, October 2019.

Costello, Matthew, and James Hawdon, "Who Are the Online Extremists Among Us? Socio-Demographic Characteristics, Social Networking, and Online Experiences of Those Who Produce Online Hate Materials," *Violence and Gender*, Vol. 5, No. 1, March 2018, pp. 55–60.

Costello, Matthew, James Hawdon, Thomas Ratliff, and Tyler Grantham, "Who Views Online Extremism? Individual Attributes Leading to Exposure," *Computers in Human Behavior*, Vol. 63, October 2016, pp. 311–320.

D'Anastasio, Cecilia, "The Christchurch Shooter and YouTube's Radicalization Trap," *Wired*, December 8, 2020.

Davey, Jacob, and Julia Ebner, *The Fringe Insurgency: Connectivity, Convergence and Mainstreaming of the Extreme Right*, London: Institute for Strategic Dialogue, 2017.

Davey, Jacob, and Julia Ebner, *"The Great Replacement": The Violent Consequences of Mainstreamed Extremism,* London: Institute for Strategic Dialogue, 2019.

Deloughery, Kathleen, Ryan D. King, and Victor Asal, "Close Cousins or Distant Relatives? The Relationship Between Terrorism and Hate Crime," *Crime & Delinquency*, Vol. 58, No. 5, October 5, 2012, pp. 663–688.

Department of Defense Instruction 1325.06, *Handling Dissident and Protest Activities Among Members of the Armed Forces*, incorporating change 1, February 22, 2012.

Department of Defense Instruction 1325.06, *Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces*, November 27, 2009, incorporating change 2, December 20, 2021.

DeVito, Michael A., "From Editors to Algorithms: A Values-Based Approach to Understanding Story Selection in the Facebook News Feed," *Digital Journalism*, Vol. 5, No. 6, 2017, pp. 753–773.

Ditto, Peter H., and David F. Lopez, "Motivated Skepticism: Use of Differential Decision Criteria for Preferred and Nonpreferred Conclusions," *Journal of Personality and Social Psychology*, Vol. 63, No. 4, 1992, pp. 568–584.

Doering, Sara, Garth Davies, and Raymond Corrado, "Reconceptualizing Ideology and Extremism: Toward an Empirically-Based Typology," *Studies of Conflict & Terrorism*, July 17, 2020.

Donovan, Joan, Becca Lewis, and Brian Friedberg, "Parallel Ports: Sociotechnical Change from the Alt-Right to Alt-Tech," in Maik Fielitz and Nick Thurston, eds., *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*, Bielefeld, Germany: transcript Verlag, 2019, pp. 49–65.

Douglas, David M., "Doxing: A Conceptual Analysis," *Ethics and Information Technology*, Vol. 18, No. 3, 2016, pp. 199–210.

Dylko, Ivan, Igor Dolgov, William Hoffman, Nicholas Eckhart, Maria Molina, and Omar Aaziz, "Impact of Customizability Technology on Political Polarization," *Journal of Information Technology & Politics*, Vol. 15, No. 1, 2018, pp. 19–33.

Ebner, Julia, "Counter-Creativity: Innovative Ways to Counter Far-Right Communication Tactics," in Maik Fielitz and Nick Thurston, eds., *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US,* Bielefeld, Germany: transcript Verlag, 2019a, pp. 169–182.

Ebner, Julia, "Replatforming Unreality," *Journal of Design and Science*, Vol. 6, September 5, 2019b.

Eddington, Patrick G., "Biden's Domestic Terrorism Strategy: A Recipe for Civil Liberties Abuses?" *CATO at Liberty*, June 15, 2021.

European Union Agency for Law Enforcement Cooperation, *European Union Terrorism Situation and Trend Report 2020*, The Hague, 2020.

Executive Office of the President, *National Strategy for Countering Domestic Terrorism*, Washington, D.C.: National Security Council and White House, June 2021.

Financial Action Task Force, *Ethnically or Racially Motivated Terrorism Financing*, Paris, France, June 2021.

Five Country Ministerial, "Joint Meeting of FCM and Quintet of Attorneys-General," London: Government of the United Kingdom, 2019.

Forscher, Patrick S., and Nour S. Kteily, "A Psychological Profile of the Alt-Right," *Perspectives on Psychological Science*, Vol. 15, No. 1, January 2020, pp. 90–116.

Frenkel, Sheera, and Davey Alba, "In India, Facebook Grapples with an Amplified Version of Its Problems," *New York Times*, October 23, 2021.

Frimer, Jeremy A., Mark J. Brandt, Zachary Melton, and Matt Motyl, "Extremists on the Left and Right Use Angry, Negative Language," *Personality and Social Psychology Bulletin*, Vol. 45, No. 8, 2019, pp. 1216–1231.

Furnell, Steven M., and Matthew J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium," *Computers & Security*, Vol. 18, No. 1, 1999, pp. 28–34.

Gallacher, John D., Marc W. Heerdink, and Miles Hewstone, "Online Engagement Between Opposing Political Protest Groups via Social Media Is Linked to Physical Violence of Offline Encounters," *Social Media + Society*, Vol. 7, No. 1, January–March 2021, pp. 1–16.

Ganesh, Bharath, and Jonathan Bright, "Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation," *Policy & Internet*, Vol. 12, No. 1, March 2020, pp. 6–19.

Garrett, R. Kelly, "Echo Chambers Online? Politically Motivated Selective Exposure Among Internet News Users," *Journal of Computer-Mediated Communication*, Vol. 14, No. 2, 2009, pp. 265–285.

Garrett, R. Kelly, Brian E. Weeks, and Rachel L. Neo, "Driving a Wedge Between Evidence and Beliefs: How Online Ideological News Exposure Promotes Political Misperceptions," *Journal of Computer-Mediated Communication*, Vol. 21, No. 5, September 2016, pp. 331–348.

Gaudette, Tiana, Ryan Scrivens, Garth Davies, and Richard Frank, "Upvoting Extremism: Collective Identity Formation and the Extreme Right on Reddit," Global Network on Extremism & Technology, November 25, 2020.

Gaudette, Tiana, Ryan Scrivens, and Vivek Venkatesh, "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists," *Terrorism and Political Violence*, July 16, 2020.

Geiß, Stefan, Melanie Magin, Pascal Jürgens, and Birgit Stark, "Loopholes in the Echo Chambers: How the Echo Chamber Metaphor Oversimplifies the Effects of Information Gateways on Opinion Expression," *Digital Journalism*, Vol. 9, No. 5, 2021, pp. 660–686.

Gendron, Angela, "The Call to Jihad: Charismatic Preachers and the Internet," *Studies in Conflict & Terrorism*, Vol. 40, No. 1, 2017, pp. 44–61.

Gerstenfeld, Phyllis B., Diana R. Grant, and Chau-Pu Chiang, "Hate Online: A Content Analysis of Extremist Internet Sites," *Analyses of Social Issues and Public Policy*, Vol. 3, No. 1, 2003, pp. 29–44.

Gielen, Amy-Jane, "Countering Violent Extremism: A Realist Review for Assessing What Works, for Whom, in What Circumstances, and How?" *Terrorism and Political Violence*, Vol. 31, No. 6, 2019, pp. 1149–1167.

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan, "Terrorist Use of the Internet by the Numbers," *Criminology & Public Policy*, Vol. 16, No. 1, February 2017, pp. 99–117.

Gill, Paul, Emily Corner, Amy Thornton, and Maura Conway, *What Are the Roles of the Internet in Terrorism? Measuring Online Behaviours of Convicted UK Terrorists*, Dublin, Ireland: VOX-Pol Network of Excellence, 2015.

Gill, Paul, John Horgan, and Paige Deckert, "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists," *Journal of Forensic Sciences*, Vol. 59, No. 2, March 2014, pp. 425–435.

Gilmer, Ellen M., "Civil Liberties Worries Loom in Plan to Identify Insider Threats," Bloomberg, June 23, 2021.

Gitari, Njagi Dennis, Zhang Zuping, Hanyurwimfura Damien, and Jun Long, "A Lexicon-Based Approach for Hate Speech Detection," *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 10, No. 4, 2015, pp. 215–230.

Goldman, Adam, and Eric Schmitt, "One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program," *New York Times*, November 24, 2016.

Graham, Robert, "How Terrorists Use Encryption," *CTC Sentinel*, Vol. 9, No. 6, June 2016, pp. 20–25.

Graham, Roderick, "Inter-Ideological Mingling: White Extremist Ideology Entering the Mainstream on Twitter," *Sociological Spectrum*, Vol. 36, No. 1, 2016, pp. 24–36.

Greenberg, Jeff, and Eva Jonas, "Psychological Motives and Political Orientation—The Left, the Right, and the Rigid: Comment on Jost et al. (2003)," *Psychological Bulletin*, Vol. 129, No. 3, 2003, pp. 376–382.

Guhl, Jakob, and Jacob Davey, *A Safe Space to Hate: White Supremacist Mobilisation on Telegram*, London: Institute for Strategic Dialogue, June 26, 2020.

Hale, W. Chris, "Extremism on the World Wide Web: A Research Review," *Criminal Justice Studies,* Vol. 25, No. 4, 2012, pp. 343–356.

Hardy, Bruce, and Dietram A. Scheufele, "Examining Differential Gains from Internet Use: Comparing the Moderating Role of Talk and Online Interactions," *Journal of Communication*, Vol. 55, No. 1, March 2005, pp. 71–84.

Hartzell, Stephanie L., "Alt-White: Conceptualizing the 'Alt-Right' as a Rhetorical Bridge Between White Nationalism and Mainstream Public Discourse," *Journal of Contemporary Rhetoric*, Vol. 8, No. 1/2, 2018, pp. 6–25.

Hassan, Ghayda, Sébastien Brouillette-Alarie, Séraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnpaul Varela, Evgueni Borokhovski, Vivek Venkatesh, Cécile Rousseau, and Stijn Sieckelinck, "Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence," *International Journal of Developmental Science*, Vol. 12, No. 1–2, 2018, pp. 71–88.

Helmus, Todd C., and Elizabeth Bodine-Baron, *Empowering ISIS Opponents on Twitter*, Santa Monica, Calif.: RAND Corporation, PE-227-RC, 2017. As of October 20, 2021: https://www.rand.org/pubs/perspectives/PE227.html

Holt, Thomas J., Joshua D. Freilich, and Steven M. Chermak, "Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures," *Deviant Behavior*, Vol. 38, No. 8, 2017, pp. 855–869.

Holt, Tom, Joshua D. Freilich, Steven Chermak, and Clark McCauley, "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos," *Dynamics of Asymmetric Conflict*, Vol. 8, No. 2, 2015, pp. 107–120.

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

Huguet, Alice, John F. Pane, Garrett Baker, Laura S. Hamilton, and Susannah Faxon-Mills, *Media Literacy Education to Counter Truth Decay: An Implementation and Evaluation Framework,* Santa Monica, Calif.: RAND Corporation, RR-A112-18, 2021. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RRA112-18.html

Institute for Strategic Dialogue and the Global Disinformation Index, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, London, October 27, 2020.

Jacobson, Michael, "Terrorist Financing and the Internet," *Studies in Conflict & Terrorism*, Vol. 33, No. 4, 2010, pp. 353–363.

Jan, Tracy, "PayPal Escalates the Tech Industry's War on White Supremacy," *Washington Post*, August 16, 2017.

Jigsaw, "Global, Connected and Decentralized," *The Current*, No. 2, 2020.

Johnson, Neil F., Rhys Leahy, Nicholas Johnson Restrepo, Nicholas Velásquez, Minzhang Zheng, Pedro Manrique, Prajwal Devkota, and Stefan Wuchty, "Hidden Resilience and Adaptive Dynamics of the Global Online Hate Ecology," *Nature*, Vol. 573, 2019, pp. 261–265.

Jost, John T., Jack Glaser, Ari W. Kruglanski, and Frank J. Sulloway, "Political Conservatism as Motivated Social Cognition," *Psychological Bulletin*, Vol. 129, No. 3, 2003, pp. 339–375.

Keatinge, Tom, Florence Keen, and Kayla Izenman, "Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It," *RUSI Journal*, Vol. 164, No. 2, 2019, pp. 10–23.

Kenyon, Jonathan, Christopher Baker-Beall, and Jens Binder, "Lone-Actor Terrorism—A Systematic Literature Review," *Studies in Conflict & Terrorism*, March 4, 2021.

Khazan, Olga, "The Far Right's Fear of 'Glowies,'" *The Atlantic*, January 25, 2021.

Killion, Victoria L., *Terrorism, Violent Extremism, and the Internet: Free Speech Considerations*, Washington, D.C.: Congressional Research Service, R45713, May 6, 2019.

King, Michael, and Donald M. Taylor, "The Radicalization of Homegrown Jihadists: A Review of Theoretical Models and Social Psychological Evidence," *Terrorism and Political Violence*, Vol. 23, No. 4, 2011, pp. 602–622.

Klausen, Jytte, "Tweeting the *Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, Vol. 38, No. 1, 2015, pp. 1–22.

Koehler, Daniel, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, No. 1, Winter 2014/2015, pp. 116–134.

Köhler, Daniel, and Julia Ebner, "Strategies and Tactics: Communication Strategies of Jihadists and Right-Wing Extremists," in Johannes Baldauf, Julia Ebner, and Jakob Guhl, eds., *Hate Speech and Radicalisation Online: The OCCI Research Report*, London: Institute for Strategic Dialogue, 2019, pp. 18–26.

Koren, James Rufus, "Can White Supremacist Groups Be Blocked from Raising Money Online? There's a Campaign to Try," *Los Angeles Times*, August 17, 2017.

Kushin, Matthew J., and Kelin Kitchener, "Getting Political on Social Network Sites: Exploring Online Political Discourse on Facebook," *First Monday*, Vol. 14, No. 11, November 2009.

Leadership Conference on Civil and Human Rights, "Leading Civil Rights Organizations Oppose Creation of New Domestic Terrorism Legislation," press release, Washington, D.C., January 19, 2021.

Ledwich, Mark, and Anna Zaitsev, "Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization," *First Monday*, Vol. 25, No. 3, March 2, 2020.

Lee, Jae Kook, Jihyang Choi, Cheonsoo Kim, and Yonghwan Kim, "Social Media, Network Heterogeneity, and Opinion Polarization," *Journal of Communication*, Vol. 64, No. 4, August 2014, pp. 702–722.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Michael Jenkins, *Countering the New Terrorism*, Santa Monica, Calif.: RAND Corporation, MR-989-AF, 1999. As of October 20, 2021: https://www.rand.org/pubs/monograph_reports/MR989.html

Levin, Brian, "Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America," *American Behavioral Scientist*, Vol. 45, No. 6, February 2002, pp. 958–988.

Levinson-Waldman, Rachel, and Sahil Singhvi, "Law Enforcement Social Media Monitoring Is Invasive and Opaque," Brennan Center for Justice, November 6, 2019.

Mackie, Diane M., Thierry Devos, and Eliot R. Smith, "Intergroup Emotions: Explaining Offensive Action Tendencies in an Intergroup Context," *Journal of Personality and Social Psychology*, Vol. 79, No. 4, 2000, pp. 602–616.

Marcellino, William, Kate Cox, Katerina Galai, Linda Slapakova, Amber Jaycocks, and Ruth Harris, *Human-Machine Detection of Online-Based Malign Information*, Santa Monica, Calif.: RAND Corporation, RR-A519-1, 2020a. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RRA519-1.html

Marcellino, William, Todd C. Helmus, Joshua Kerrigan, Hilary Reininger, Rouslan I. Karimov, and Rebecca Ann Lawrence, *Detecting Conspiracy Theories on Social Media: Improving Machine Learning to Detect and Understand Online Conspiracy Theories*, Santa Monica, Calif.: RAND Corporation, RR-A676-1, 2021. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RRA676-1.html

Marcellino, William, Madeline Magnuson, Anne Stickells, Benjamin Boudreaux, Todd C. Helmus, Edward Geist, and Zev Winkelman, *Counter-Radicalization Bot Research: Using Social Bots to Fight Violent Extremism*, Santa Monica, Calif.: RAND Corporation, RR-2705-DOS, 2020b. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RR2705.html

McCauley, Clark, and Sophia Moskalenko, "Mechanisms of Political Radicalization: Pathways Toward Terrorism," *Terrorism and Political Violence*, Vol. 20, No. 3, 2008, pp. 415–433.

McPherson, Miller, Lynn Smith-Lovin, and James M. Cook, "Birds of a Feather: Homophily in Social Networks," *Annual Review of Sociology*, Vol. 27, August 2001, pp. 415–444.

Meleagrou-Hitchens, Alexander, Audrey Alexander, and Nick Kaderbhai, "The Impact of Digital Communications Technology on Radicalization and Recruitment," *International Affairs*, Vol. 93, No. 5, September 2017, pp. 1233–1249.

Meleagrou-Hitchens, Alexander, and Nick Kaderbhai, *Research Perspectives on Online Radicalisation: A Literature Review, 2006–2016*, Dublin, Ireland: VOX-Pol Network of Excellence, 2017.

Merchant, Nomaan, "US to Ramp Up Tracking of Domestic Extremism on Social Media," Associated Press, May 20, 2021.

Merrill, Jeremy B., and Will Oremus, "Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation," *Washington Post*, October 26, 2021.

Mettler, Katie, and Avi Selk, "GoDaddy—Then Google—Ban Neo-Nazi Site Daily Stormer for Disparaging Charlottesville Victim," *Washington Post*, August 14, 2017.

Mills, Colleen, Joshua D. Freilich, Steven M. Chermak, Thomas J. Holt, and Gary LaFree, "Social Learning and Social Control in the Off- and Online Pathways to Hate Crime and Terrorist Violence," *Studies in Conflict & Terrorism*, Vol. 44, No. 8, 2021, pp. 701–729.

Mitts, Tamar, "Banned: How Deplatforming Extremists Mobilizes Hate in the Dark Corners of the Internet," conference paper, National Bureau of Economic Research Summer Institute, July 26, 2021.

Mondal, Mainack, Leandro Araújo Silva, and Fabrício Benevenuto, "A Measurement Study of Hate Speech in Social Media," *HT '17: Proceedings of the 28th ACM Conference on Hypertext and Social Media*, July 2017, pp. 85–94.

Mondon, Aurelien, and Aaron Winter, "Racist Movements, the Far Right and Mainstreaming," in John Solomos, ed., *Routledge International Handbook of Contemporary Racisms*, Abingdon, United Kingdom: Routledge, 2020.

Muldowney, Decca, "Info Wars: Inside the Left's Online Efforts to Out White Supremacists," ProPublica, October 30, 2017.

Müller, Karsten, and Carlo Schwarz, "Fanning the Flames of Hate: Social Media and Hate Crime," *Journal of the European Economic Association*, Vol. 19, No. 4, August 2021, pp. 2132–2167.

Munn, Luke, "Alt-Right Pipeline: Individual Journeys to Extremism Online," *First Monday*, Vol. 24, No. 6, June 3, 2019.

Munn, Luke, "Angry by Design: Toxic Communication and Technical Architectures," *Humanities and Social Sciences Communications*, Vol. 7, No. 53, 2020, pp. 1–11.

Nesser, Petter, Anne Stenersen, and Emilie Oftedal, "Jihadi Terrorism in Europe: The IS-Effect," *Perspectives on Terrorism*, Vol. 10, No. 6, December 2016, pp. 3–24.

Neumann, Peter, *Countering Online Radicalization in America*, Washington, D.C.: Bipartisan Policy Center, December 2012.

Neumann, Peter, and Scott Kleinmann, "How Rigorous Is Radicalization Research?" *Democracy and Security*, Vol. 9, No. 4, 2013, pp. 360–382.

Neumann, Peter R., "The Trouble with Radicalization," *International Affairs*, Vol. 89, No. 4, 2013, pp. 873–893.

Nienierza, Angela, Carsten Reinemann, Nayla Fawzi, Claudia Riesmeyer, and Katharina Neumann, "Too Dark to See? Explaining Adolescents' Contact with Online Extremism and Their Ability to Recognize It," *Information, Communication & Society*, Vol. 24, No. 9, 2021, pp. 1229–1246.

Nuori, Lella, Nuria Lorenzo-Dus, and Amy-Louise Watkin, "Following the Whack-a-Mole: Britain First's Visual Strategy from Facebook to Gab," London: Royal United Services Institute for Defence and Security Studies, Global Research Network on Terrorism and Technology Paper No. 4, July 4, 2019.

Office of the Director of National Intelligence, "Domestic Violent Extremism Poses Heightened Threat in 2021," unclassified summary, Washington, D.C., March 1, 2021.

Onursal, Recep, and Daniel Kirkpatrick, "Is Extremism the 'New' Terrorism? The Convergence of 'Extremism' and 'Terrorism' in British Parliamentary Discourse," *Terrorism and Political Violence*, Vol. 33, No. 5, 2021, pp. 1094–1116.

Paris Peace Forum, "Digital Platforms and Extremism: Are Content Controls Effective?" in *Insights from the 2018 Paris Peace Forum Debate Sessions*, November 13, 2018.

Pauwels, Lieven, and Nele Schils, "Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives," *Terrorism and Political Violence*, Vol. 28, No. 1, 2016, pp. 1–29.

Post, Jerrold M., "Terrorism and Right-Wing Extremism: The Changing Face of Terrorism and Political Violence in the 21st Century: The Virtual Community of Hatred," *International Journal of Group Psychotherapy*, Vol. 65, No. 2, 2015, pp. 242–271.

Post, Jerrold M., Cody McGinnis, and Kristen Moody, "The Changing Face of Terrorism in the 21st Century: The Communications Revolution and the Virtual Community of Hatred," *Behavioral Sciences and the Law*, Vol. 32, No. 3, May–June 2014, pp. 306–334.

Price, Ned, "United States Joins Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online," press statement, Washington, D.C.: U.S. Department of State, May 7, 2021.

Prucha, Nico, and Ali Fisher, "Tweeting for the Caliphate: Twitter as the New Frontier for Jihadi Propaganda," *CTC Sentinel,* Vol. 6, No. 6, June 2013, pp. 19–23.

Ravndal, Jacob Aasland, and Tore Bjørgo, "Investigating Terrorism from the Extreme Right: A Review of Past and Present Research," *Perspectives on Terrorism*, Vol. 12, No. 6, December 2018, pp. 5–22.

Rhoades, Ashley L., Todd C. Helmus, James V. Marrone, Victoria Smith, and Elizabeth Bodine-Baron, *Promoting Peace as the Antidote to Violent Extremism: Evaluation of a Philippines-Based Tech Camp and Peace Promotion Fellowship*, Santa Monica, Calif.: RAND Corporation, RR-A233-3, 2020. As of October 20, 2021: https://www.rand.org/pubs/research_reports/RRA233-3.html

Ribeiro, Manoel Horta, Raphael Ottoni, Robert West, Virgílio A. F. Almeida, and Wagner Meira, Jr., "Auditing Radicalization Pathways on YouTube," *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 2020, pp. 131–141.

Richards, Anthony, "From Terrorism to 'Radicalization' to 'Extremism': Counterterrorism Imperative or Loss of Focus?" *International Affairs*, Vol. 91, No. 2, March 2015, pp. 371–380.

Riek, Blake M., Eric W. Mania, and Samuel L. Gaertner, "Intergroup Threat and Outgroup Attitudes: A Meta-Analytic Review," *Personality and Social Psychology Review*, Vol. 10, No. 4, 2006, pp. 336–353.

Röchert, Daniel, Muriel Weitzel, and Björn Ross, "The Homogeneity of Right-Wing Populist and Radical Content in YouTube Recommendations," *Proceedings of the SMSociety '20: International Conference on Social Media and Society*, July 2020, pp. 245–254.

Rogers, Richard, "Deplatforming: Following Extreme Internet Celebrities to Telegram and Alternative Social Media," *European Journal of Communication*, Vol. 35, No. 3, 2020, pp. 213–229.

Roose, Kevin, "The Making of a YouTube Radical," *New York Times*, June 8, 2019.

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

Schafer, Joseph A., "Spinning the Web of Hate: Web-Based Hate Propagation by Extremist Organizations," *Journal of Criminal Justice and Popular Culture*, Vol. 9, No. 2, 2002, pp. 69–88.

Schmid, Alex, "Violent and Non-Violent Extremism: Two Sides of the Same Coin?" The Hague: International Centre for Counter-Terrorism, May 2014.

Schuurman, Bart, "Topics in Terrorism Research: Reviewing Trends and Gaps, 2007–2016," *Critical Studies in Terrorism*, Vol. 12, No. 3, 2019, pp. 463–480.

Sedgwick, Mark, "The Concept of Radicalization as a Source of Confusion," *Terrorism and Political Violence*, Vol. 22, No. 4, 2010, pp. 479–494.

Shehabat, Ahmad, and Teodor Mitew, "Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics," *Perspectives on Terrorism*, Vol. 12, No. 1, February 2018, pp. 81–99.

Silber, Mitchell D., and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York: New York City Police Department, 2007.

Simi, Pete, and Robert Futrell, "Cyberculture and the Endurance of White Power Activism," *Journal of Political and Military Sociology*, Vol. 34, No. 1, Summer 2006, pp. 115–142.

Simi, Pete, and Robert Futrell, *American Swastika: Inside the White Power Movement's Hidden Spaces of Hate*, Lanham, Md.: Rowman & Littlefield, 2010.

Simi, Pete, Steven Windisch, and Karyn Sporer, *Recruitment and Radicalization Among US Far-Right Terrorists*, College Park, Md.: National Consortium for the Study of Terrorism and Responses to Terrorism, November 2016.

Sinai, Joshua, with Jeffrey Fuller and Tiffany Seal, "Research Note: Effectiveness in Counter-Terrorism and Countering Violent Extremism: A Literature Review," *Perspectives on Terrorism*, Vol. 13, No. 6, December 2019, pp. 90–108.

Singh, Spandana, *Everything in Moderation: An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User-Generated Content*, Washington, D.C.: New America, July 15, 2019.

Smith, Allison G., *How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us*, Washington, D.C.: U.S. Department of Justice, June 2018.

Smith, Laura, "Lone Wolves Connected Online: A History of Modern White Supremacy," *New York Times*, January 26, 2021.

Spears, Russell, Martin Lea, and Stephen Lee, "De-Individuation and Group Polarization in Computer-Mediated Communication," *British Journal of Social Psychology*, Vol. 29, No. 2, June 1990, pp. 121–134.

Statt, Nick, "Apple Pay Is Dropping Support for Websites That Sell White Supremacist Merchandise," *The Verge*, August 16, 2017.

Stephens, William, Stijn Sieckelinck, and Hans Boutellier, "Preventing Violent Extremism: A Review of the Literature," *Studies in Conflict & Terrorism*, Vol. 44, No. 4, 2021, pp. 346–361.

Stroud, Natalie Jomini, "Polarization and Partisan Selective Exposure," *Journal of Communication*, Vol. 60, No. 3, 2010, pp. 556–576.

Suler, John, "The Online Disinhibition Effect," *International Journal of Applied Psychoanalytic Studies*, Vol. 2, No. 2, June 2005, pp. 184–188.

Sunstein, Cass R., *Republic.com*, Princeton, N.J.: Princeton University Press, 2001.

Sunstein, Cass R., "The Law of Group Polarization," *Journal of Political Philosophy*, Vol. 10, No. 2, 2002, pp. 175–195.

Sweeney, Matthew M., and Arie Perliger, "Explaining the Spontaneous Nature of Far-Right Violence in the United States," *Perspectives on Terrorism*, Vol. 12, No. 6, December 2018, pp. 52–71.

Tai, Kuang-Ting, Gregory Porumbescu, and Jongmin Shon, "Can E-Participation Stimulate Offline Citizen Participation: An Empirical Test with Practical Implications," *Public Management Review*, Vol. 22, No. 2, 2020, pp. 278–296.

Thomas, Timothy L., "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters*, Vol. 23, No. 1, Spring 2003, pp. 112–123.

Torres-Soriano, Manuel R., "Barriers to Entry to Jihadist Activism on the Internet," *Studies in Conflict & Terrorism*, 2021.

Tsfati, Yariv, and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict & Terrorism*, Vol. 25, No. 5, 2002, pp. 317–332.

United Nations Office of Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, New York, 2012.

United Nations Security Council, Counter-Terrorism Committee, Executive Directorate, "CTED Launches Trends Alert on 'Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism,'" press release, New York, April 1, 2020.

United Nations Security Council Resolution 2395, December 21, 2017.

United Nations Security Council Resolution 2396, December 21, 2017.

Urman, Aleksandra, and Stefan Katz, "What They Do in the Shadows: Examining the Far-Right Networks on Telegram," *Information, Communication & Society*, 2020.

U.S. Department of Homeland Security, *Homeland Threat Assessment*, Washington, D.C., October 2020.

U.S. Department of Justice, "International Statement: End-to-End Encryption and Public Safety," press release, Washington, D.C., October 11, 2020.

U.S. House of Representatives, Committee on Oversight and Government Reform, *Radicalization: Social Media and the Rise of Terrorism*, hearing before the Subcommittee on National Security, Washington, D.C., October 28, 2015.

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

Veldhuis, Tinka, and Jørgen Staun, *Islamist Radicalisation: A Root Cause Model*, The Hague: Netherlands Institute of International Relations Clingendael, October 2009.

Vergani, Matteo, Muhammad Iqbal, Ekin Ilbahar, and Greg Barton, "The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence About Radicalization into Violent Extremism," *Studies in Conflict & Terrorism*, Vol. 43, No. 10, 2020, pp. 854–885.

Von Behr, Ines, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, Santa Monica, Calif., and Cambridge, United Kingdom: RAND Corporation, 2013. As of August 11, 2021: https://www.rand.org/pubs/research_reports/RR453.html

Wahlström, Mattias, and Anton Törnberg, "Social Media Mechanisms for Right-Wing Political Violence in the 21st Century: Discursive Opportunities, Group Dynamics, and Co-Ordination," *Terrorism and Political Violence*, Vol. 33, No. 4, 2021, pp. 766–787.

Walther, Samantha, and Andrew McCoy, "US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism," *Perspectives on Terrorism*, Vol. 15, No. 2, April 2021, pp. 100–124.

Weimann, Gabriel, *www.terror.net: How Modern Terrorism Uses the Internet*, Washington, D.C.: United States Institute of Peace, special report 116, March 2004.

Weimann, Gabriel, "Lone Wolves in Cyberspace," *Journal of Terrorism Research*, Vol. 3, No. 2, Autumn 2012, pp. 75–90.

Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation*, Washington, D.C.: Woodrow Wilson Center Press, 2015.

Weinberg, Leonard, Ami Pedahzur, and Sivan Hirsch-Hoefler, "The Challenges of Conceptualizing Terrorism," *Terrorism and Political Violence*, Vol. 16, No. 4, 2004, pp. 777–794.

White House, "Statement by Press Secretary Jen Psaki on the Occasion of the United States Joining the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online," press statement, May 7, 2021.

Whittaker, Joe, Seán Looney, Alastair Reed, and Fabio Votta, "Recommender Systems and the Amplification of Extremist Content," *Internet Policy Review*, Vol. 10, No. 2, 2021.

Wiktorowicz, Quintan, "Working to Counter Online Radicalization to Violence in the United States," White House, archive, February 5, 2013.

Williams, Heather J., Alexandra T. Evans, Jamie Ryan, Erik E. Mueller, and Bryce Downing, *The Online Extremist Ecosystem: Its Evolution and a Framework for Separating Extreme from Mainstream*, Santa Monica, Calif.: RAND Corporation, PE-A1458-1, 2021. As of December 2, 2021: https://www.rand.org/pubs/perspectives/PEA1458-1.html

Williams, Matthew L., Pete Burnap, Amir Javed, Han Liu, and Sefa Ozalp, "Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime," *British Journal of Criminology*, Vol. 60, No. 1, January 2020, pp. 93–117.

Windle, James, "Fundraising, Organised Crime and Terrorist Financing," in Andrew Silke, ed., *Routledge Handbook of Terrorism and Counterterrorism*, Abingdon, United Kingdom: Routledge, 2019, pp. 195–206.

Winter, Charlie, *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*, London: Qulliam, 2015.

Wojcieszak, Magdalena, "'Carrying Online Participation Offline'—Mobilization by Radical Online Groups and Politically Dissimilar Offline Ties," *Journal of Communication*, Vol. 59, No. 3, 2009, pp. 564–586.

Wojcieszak, Magdalena, "'Don't Talk to Me'—Effects of Ideologically Homogeneous Online Groups and Politically Dissimilar Offline Ties on Extremism," *New Media & Society*, Vol. 12, No. 4, 2010, pp. 637–655.

Woodruff Swan, Betsy, "Biden's Domestic Terrorism Strategy Concerns Advocates," *Politico,* July 22, 2021.

Wray, Christopher, "Worldwide Threats to the Homeland," statement before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., September 24, 2020.

Yachot, Noa, "Fears Grow That Efforts to Combat US Domestic Terrorism Can Hurt Minorities," *The Guardian*, January 26, 2021.

Youngblood, Mason, "Extremist Ideology as a Complex Contagion: The Spread of Far-Right Radicalization in the United States Between 2005 and 2017," *Humanities and Social Sciences Communications,* Vol. 7, No. 49, July 31, 2020.

Zhuravskaya, Ekaterina, Maria Petrova, and Ruben Enikolopov, "Political Effects of the Internet and Social Media," *Annual Review of Economics*, Vol. 12, August 2020, pp. 415–438.

Zuckerman, Ethan, and Chand Rajendra-Nicolucci, "Deplatforming Our Way to the Alt-Tech Ecosystem," Knight First Amendment Institute at Columbia University, January 11, 2021.

Photo credits

Cover texture: JNBgraphics/iStock/Getty

Page iv background texture: JNBgraphics/iStock/Getty

Page 1: Illustration by Jessica Arana from Sean Rayford/Alamy; dem10/Getty Images; sestovic/Getty Images; Dilok Klaisataporn/Getty Images; Comstock/Getty Images

Page 4: background texture: vural/Getty Images; Icons: Fourleaflover/Getty Images; appleuzr/Getty Images; goodvector/Getty Images

Page 7: da-vooda/Getty Images

Page 10: sestovic/Getty Images; dem10/Getty Images; da-Dilok Klaisataporn/Getty Images; eyepark/Getty Images; JNBgraphics/iStock/Getty; vooda/Getty Images

ABOUT THE AUTHORS

Alexandra T. Evans is an associate policy researcher at the RAND Corporation. Her work focuses on defense and security issues, with an emphasis on decisionmaking, scenario analysis, and threat assessment. Evans has a Ph.D. in history.

Heather J. Williams is a senior policy researcher at the RAND Corporation. Her research focuses on violent extremism and targeted violence, Middle East regional issues, and intelligence policy and methodology. Williams has an M.S. in strategic intelligence.

ABOUT THIS PERSPECTIVE

Recent demonstrations and violent attacks have highlighted the need for an improved understanding of the role of internet-based technologies in aiding and amplifying the spread of extremist ideologies. Since the early days of the internet, radical groups and movements across the ideological spectrum have demonstrated their intent and ability to harness virtual platforms to perform critical functions. This Perspective, the second in a RAND Corporation series on online white-supremacist and violent misogynist material, provides a primer on how the internet influences the activities of extremist groups and movements and how exposure to or consumption of extremist content online influences the behavior of internet users.

The research reported here was completed in December 2021.

Acknowledgments

We are thankful to RAND for providing the support and resources to conduct this effort. Jessica Arana contributed her extraordinary design skills, and Amanda Wilson managed the publication process. Conversations with Bryce Downing, Brian Mills, Caitlin McCulloch, Erik Mueller, and Jamie Ryan clarified several points and introduced us to new scholarship. We are also grateful to two reviewers, our RAND colleague Pauline Moore and Seamus Hughes, Deputy Director of the Program on Extremism at George Washington University, whose insightful comments and suggestions improved this Perspective.

RAND National Security Research Division

This research was conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Funding

Funding for this research was made possible by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

About This Perspective

Recent demonstrations and violent attacks have highlighted the need for an improved understanding of the role of internet-based technologies in aiding and amplifying the spread of extremist ideologies. Since the early days of the internet, radical groups and movements across the ideological spectrum have demonstrated their intent and ability to harness virtual platforms to perform critical functions.

This Perspective, the second in a RAND Corporation series on online white-supremacist and violent misogynist material, provides a primer on how the internet influences the activities of radical groups and movements and how exposure to or consumption of extremist content online influences the behavior of internet users. After briefly discussing relevant terminology, the authors describe the role of the internet in facilitating five operational functions for radical groups and movements: (1) group financing; (2) networking and coordination; (3) recruitment and radicalization; (4) inter- and intra-group knowledge transfer; and (5) planning, coordination, and execution of harmful online and offline operations. The authors then examine how virtual interactions can facilitate or encourage users' adoption of extremist ideas and inspire or alter offline behavior. The Perspective concludes with a discussion of how the internet can be leveraged as a tool to counter extremism, and the authors provide suggestions for further research.

www.rand.org

$24.00

ISBN-10 1-9774-0840-0
ISBN-13 978-1-9774-0840-2

PE-A1458-2