HOW EXTREMISM OPERATES ONLINE

A Primer

ALEXANDRA T. EVANS AND HEATHER J. WILLIAMS
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. 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.”

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. 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. 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 non-violent 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-
HOW EXTREMISM OPERATES ONLINE

Financing and fundraising functions illustrate how extremists can use internet-based tools to mimic activities that are traditionally performed in physical spaces. 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. 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. 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.

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. 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.

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. Yet, for larger

---

**FIGURE 1**

### FINANCING
- Direct solicitation of donations
- Crowdfunding
- Advertisement of needs
- Merchandise sales
- E-commerce

### NETWORKING AND COORDINATION
- Social networking
- Advertisement of offline activities
- Encouragement and direction
- Conduits for private and mass communication

### RECRUITMENT AND RADICALIZATION
- Creation and dissemination of propaganda
- Broadcast of message to global audiences
- Direct, secure communication with potential recruits

### KNOWLEDGE TRANSFER
- Creation, dissemination, and storage of text, video, and visual training materials
- Facilitation of inter-group networking and exchange

### MOBILIZATION TO ACTION
- Surveillance and intelligence on targets
- Planning, coordination, and execution of online tactics (e.g., doxxing, swarming, cyberbullying)
- Planning and advertisement of offline action (e.g., demonstrations, violent attacks)
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. 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. 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.

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. 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. 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.

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.

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.

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.”

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.

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. 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. 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. 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. “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.”

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.
HOW EXTREMISM OPERATES ONLINE
and fostering group identification—dynamics that, in turn, increase users’ susceptibility to more-extreme positions.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.”

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. 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.”

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. These findings align with suggestive evidence that increased participation in virtual extremist communities corresponds with changes in offline behavior. 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.

Others have suggested that consumption of virtual propaganda may encourage adherents of extremist groups to translate grievances into violent action. 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. “[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.”

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.” 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. 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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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. 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. 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.

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. 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.

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. 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. Disagreements over how to define hate speech also present barriers to designing effective tools to detect and disrupt extremist behavior online.

Moreover, researchers generally agree that addressing the underlying drivers of extremism requires effective counternarrative messaging and community programming. 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.

Disagreements over who should produce and disseminate counternarratives also present an impediment to designing and implementing new programs. 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-
individual 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. 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. 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
- 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

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. 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.** 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. 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. 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. 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. 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.


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).

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.

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).


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.

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.


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).


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

White supremacists, anti-immigration groups, and antigovernment 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).


For a review of recent literature on online recruitment, see Ana-Maria Bluic, 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.


For a similar finding, see Koehler, 2014/2015, p. 118.

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).


Decca Muldowney, “Info Wars: Inside the Left’s Online Efforts to Out White Supremacists,” ProPublica, October 30, 2017;

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).


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).


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

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

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).


Brown et al., 2021, pp. xv, 87.


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.


Brown et al., 2021, p. 19.

Youngblood, 2020, p. 1.

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.


Pauwels and Schils, 2016.


Gill et al., 2017, p. 114.

Gill et al., 2017, p. 114.


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.:


“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.


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


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**


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.


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 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