Extremist Use of Online Spaces

Heather J. Williams and Alexandra T. Evans
Extremist Use of Online Spaces

Testimony of Heather J. Williams and Alexandra T. Evans

The RAND Corporation

Before the Select Committee to Investigate the January 6th Attack on the United States Capitol
United States House of Representatives

April 25, 2022

Extremists—be they motivated by racial, ethnic, or religious prejudice or anti-government sentiment—have used the internet since its early days. The internet provides a low-cost mechanism for these individuals and groups to extend their reach and finance their activities, network with like-minded individuals, recruit new members, share knowledge among themselves, and coordinate operational activities. Extremist content can be found in all corners of the web: on message forums, social networking platforms, streaming services, live chats of video games, static websites, and encrypted communication applications. Characterizing and quantifying the variety and volume of extremist use of such virtual platforms is difficult given the nature of these online spaces themselves. Social media and messaging platforms shift in popularity, are often opaque in their operation, and frequently are designed to ensure users’ anonymity. Platform operators provide limited data to the public and to researchers about either their users or their operating algorithms in general; even less is known about how extremists specifically use these platforms to further their causes.3

In this statement, we extrapolate from findings of earlier research on the online extremist ecosystem to examine how the internet may have helped foster conditions that contributed to the

1 The opinions and conclusions expressed in this testimony are the authors’ alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

2 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. RAND’s mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

attack on the U.S. Capitol complex on January 6, 2021. Although the United States has experienced waves of violent extremism since its founding, and although some of the ideas espoused by the far-right extremists that participated in the attack predate the invention of the internet, such mob events in U.S. history have been rare. Existing research conducted at RAND and elsewhere suggests that online spaces may have fueled the spread of conspiracy theories and disinformation—in this case, related to false claims of election fraud in the 2020 presidential election—and provided extremists with new mechanisms to reach potentially receptive audiences. Moreover, online spaces have become incubators for a vicious, reinforcing cycle of polarization and propaganda. The events of January 6 demonstrated how dangerous this combination can be—and very little has changed since then to prevent those with an extreme agenda from reaching a broad audience or organizing conspiracies oriented toward undercutting American democracy.

We first briefly define far-right extremism, then survey the historical evolution of extremist activity online, focusing on why and how far-right extremists have used digital platforms. Next, we discuss how the characteristics of online spaces may have contributed to individual radicalization and enabled the formation of a mass movement based on false ideas about the November 2020 election. In the concluding section, we reflect on the status of online extremist organizing since January 6 and the prospects for another, similar attack.

We use the term far-right extremism to refer to a shifting community of individuals and groups that espouse ideologies characterized by racial, ethnic, or nationalist supremacism; a belief that social inequality is natural or desirable; and support of conspiracy theories involving grave threats to national sovereignty, personal liberty, or a national or community way of life. The term includes neo-Nazis and other white supremacist movements; anti-government activists and violent militias; and those that advance ideological agendas based on bias related to religion, gender, sexual orientation, or immigration status. The boundaries between these groups and movements are often fluid. Individual far-right activists and groups often pick and choose between (and within) varied ideological traditions, and their adherence to specific movements or tenets may not always be ideologically consistent. The U.S. government typically defines these movements as a type of domestic terrorism or domestic violent extremism and employs the terms racially or ethnically motivated violent extremists and anti-government or anti-authority violent extremists (specifically, militia violent extremists) to refer to the individuals who subscribe to these ideologies. Given the convergence between these movements, and the fact that they use online spaces similarly, we have opted to use the broader and more common term far-right extremism.

---


5 Williams et al., 2021.

Like other extremist movements, far-right networks use online platforms for a variety of functions. One is to fundraise and finance their online and offline activities. They do so on websites, social media platforms, email distribution lists, messaging apps, and other virtual tools through which they can publicize their needs, direct potential donors to traditional and online payment options, and advertise merchandise for sale. Extremists may solicit funds by simply posting requests for donations in an arena where supporters already congregate or by using crowdfunding websites and donation applications. Mainstream crowdfunding platforms, such as Indiegogo and GoFundMe, have attempted to deny service to white supremacist, anti-immigration, and anti-government groups and militias, diverting some of this activity to purpose-built platforms, such as GoyFundMe, Hatreon, and WeSearcher, that offer more-receptive environments. E-commerce is another revenue stream for far-right groups. Online retail platforms and payment-processing architecture 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 music-streaming services (e.g., Spotify or iTunes) that serve the dual purpose of disseminating radical ideas.\(^7\)

The internet has also provided right-wing extremists with a cheap, efficient, and safe way to communicate and network, while providing the impression that a movement has attracted a substantial supporter base.\(^8\) Through online platforms, far-right activists can identify and recruit potential new members to their movements. They can also easily share information and connect geographically distributed users.\(^9\) Social media, encrypted communication channels, and other like platforms can also connect individuals who live in close proximity and can facilitate offline activity by helping individuals find, communicate, and arrange meetings with others.\(^10\) One study

---


8 Evans and Williams, 2022, pp. 5–6.


of former white supremacist skinheads observed that a third of those interviewed reported that virtual interactions had enabled their first face-to-face interactions with other extremists.\(^{11}\)

Online spaces also enable the transfer of knowledge and facilitate operational coordination. Using free or low-cost streaming services, file storage platforms, and end-to-end encrypted communication applications, extremists can quickly and easily share information across the world.\(^{12}\) Far-right and white supremacist groups have shared operational manuals and training guides online, alongside racist biographies, manifestos, and other written works, between existing group members and to persuade potential or new supporters that their agendas are well established.\(^{13}\) The internet can lower the bar for exposure to these types of materials, allowing individuals to engage privately or anonymously whenever and wherever they prefer.

Ultimately, extremists largely use the same platforms for the same purposes as an average internet user. Moreover, they have learned from decades of experience and adjusted their tactics in response to new internet trends, technologies, and content policies. Far-right extremists have used online platforms since the advent of computer networks in the early 1980s, when white supremacists established public bulletin board systems (BBSs). BBS networks and then the World Wide Web helped these movements build transnational linkages and provide information to sympathetic individuals in countries where such literature was banned, such as Germany and Canada.\(^{14}\) In 1995, former Ku Klux Klan (KKK) leader Don Black set up the white supremacist forum Stormfront, which openly describes itself as a white nationalist forum and continues to operate today.\(^{15}\)

As the internet developed, extremists began to organize across both popular mainstream and dedicated niche platforms. During the period of transition sometimes described as Web 2.0—when the internet shifted to primarily user-generated content rather than static content produced by webpage publishers and designed for individual end users—extremist activity evolved in line with broader trends in internet use. Far-right users operated openly on mainstream platforms like MySpace, Facebook, YouTube, and Twitter.\(^{16}\) This activity garnered little attention outside far-
right communities until the July 2011 attack in Norway, in which a far-right extremist killed 77 people and injured hundreds. Prior to his act of violence, the perpetrator emailed his manifesto to two prominent Stormfront members, who circulated it online. He later stated that his violent act was a “marketing method” to draw attention to his manifesto and the racist, xenophobic messages within it.17

Concurrently, far-right extremists adopted virtual harassment techniques developed in the anonymous troll-and-raid culture that emerged on social networking and discussion platforms during this period, which sought to cause confusion or harm to online users without provocation or purpose beyond amusement or manipulation. By 2015, online harassment—and the media scrutiny it garnered—prompted social media platforms to take a more purposeful approach to content harassment broadly, not specifically related to far-right activity. European regulators also started pressuring technology companies to crack down on malign use of their platforms, and the European Commission published a “Code of Conduct on Countering Illegal Hate Speech Online” that encouraged the removal of racist and xenophobic hate speech online.18 Social media platforms began introducing new content moderation policies and features intended to block users from posting and viewing hateful and abusive content, although efforts were typically haphazard, reactive, and limited.

These efforts to clamp down on extremist exploitation of the internet were also mitigated by the establishment of new alternative technology or “alt-tech” platforms—such as Voat and Gab—that mimicked the functionality of mainstream social media platforms but employed more-permissive content moderation policies. These new platforms catered to individuals who had been removed or censored by mainstream platforms.19 Moreover, far-right extremists were not the principal target for social media regulators. Instead, government and private-sector initiatives were tailored to counter the Islamic State in Iraq and Syria, which was actively and effectively using online spaces to raise revenue, recruit foreign fighters, and direct terrorist attacks around the world.20 In 2017, online powerhouses Facebook, Microsoft, Twitter, and Google (which operates YouTube) established the Global Internet Forum to Counter Terrorism.21 Technology companies, working with foreign partners and the U.S. government, worked to implement safeguards, disrupt extremist organizing, and promote counter-radicalization messaging, but they


focused specifically on Islamist extremists. Far-right extremists, meanwhile, were still using online spaces to organize mass demonstrations, establish small militant cells, and inspire individual acts of violence.

Technology companies paid greater attention to far-right organizing on their platforms after the Unite the Right rally in August 2017 in Charlottesville, Virginia. This event, which attempted to coalesce alt-right, neo-Nazi, militia, neo-confederate, KKK, and other far-right organizations and sympathizers into a coherent movement, ended with the death of one person and injuries to 35 others after a neo-Nazi purposefully drove their car into a crowd of counterprotesters. In the aftermath, criticism of Twitter’s role in facilitating the event prompted the company to announce “new rules to reduce hateful conduct and abusive behavior.” Likewise, Facebook began to restrict and remove pages related to the rally and the associated violence, and Discord, a gaming-oriented text and voice chat platform, started banning far-right servers and accounts. Several website building and hosting companies, such as Squarespace, started removing white supremacist sites, and Apple and PayPal began to remove and deny white supremacist entities from using their payment-processing platforms.

In practice, however, these restrictions were only temporary obstacles for the many extremist users who proved able to either circumvent restrictions (such as by using coded speech) or find viable alternative platforms to propagate extremist sentiment. Violent attacks by far-right extremists rose in the years following the Charlottesville protests, and some perpetrators continued sharing manifestos online to try to gain infamy and inspire or incite future violence. These events often prompted technology companies to introduce new restrictions or to deny service to extremist communities, but the resulting policy changes were often unclear, unevenly enforced, and unresponsive to changes in extremist messaging or tactics. For example, Gab lost services of its domain registrar and hosting service after one of its antisemitic users posted an extremist manifesto hours before attacking the Tree of Life synagogue in Pittsburgh.

---


Pennsylvania, on October 27, 2018, an attack that killed 11 people and injured six. Despite the interruption, Gab was back online within a week.29

The events of January 6, 2021, occurred against this backdrop. The fragmented and reactive nature of the existing content moderation environment provided a favorable environment for those seeking to mobilize a mob for seditious purposes.30 Because content moderation and removal policies focused on explicitly violent speech, and because extremist groups had learned over several years how to circumvent existing restrictions and how to leverage more-permissive platforms, they were prepared to mobilize effectively on a large scale and without significant disruption. Organizers also benefited from the fact that a large number of internet users had already familiarized themselves with free and low-cost encrypted communication applications, in part because of real and anticipated experiences of deplatforming in the past. As was widely reported at the time, far-right extremists and activists openly mobilized under the “Stop the Steal” slogan on major social networks, messaging apps, and forums, including Gab, Parler, Telegram, Facebook, and TheDonald.win, for weeks prior to the attack. This activity included coded and non-coded discussion of specific plans to storm the U.S. Capitol.31 Most of the efforts by social media platforms to mitigate the spread of misinformation related to the election or associated with the QAnon mass delusion came only after January 6.32

Viewed from this longer perspective, the events of January 6 appear as one episode in a multi-decade pattern of extremist exploitation and experimentation with online tools. But what distinguished this attack from previous extremist incidents was that organizers successfully mobilized a mob and incited violent action. While the United States has previously confronted movements that demonstrated the intent and ability to organize violent group action, few have garnered an active following of this size.33 Although not the only factor, the internet played a critical role in enabling the creation of a mass movement based on false ideas about the November 2020 election.

30 Evans and Williams, 2022, pp. 8–13.
32 Brakkton Booker, “Facebook Removes ‘Stop the Steal’ Content; Twitter Suspends QAnon Accounts,” NPR, January 12, 2021.
33 An April 2021 study based on opinion polling conducted in the months after the attack on the U.S. Capitol complex estimated the size of the “core insurrectionist mobilization base” as 4 percent of the U.S. population, or approximately 10 million people (Robert A. Pape, “Understanding American Domestic Terrorism: Mobilization Potential and Risk Factors of a New Threat Trajectory,” presentation slides, Chicago, Ill.: University of Chicago, April 6, 2021). A subsequent Monmouth University poll, released in June 2021, reported that 32 percent of Americans “continue to believe that Joe Biden’s victory in 2020 was due to voter fraud – a number that has not budged since the November election” (Monmouth University Polling Institute, “Public Supports Both Early Voting and Requiring Photo ID to Vote,” webpage, June 21, 2021, https://www.monmouth.edu/polling-institute/reports/monmouthpoll_us_062121/).
Existing research also shows 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. Research further suggests that exposure to extremist communities and content online may encourage the adoption of radical norms, ideas, and behavior that extend into offline spaces. That virtual interactions can inspire or encourage the adoption of extremist beliefs is not limited to the far right and is well documented in court records, interviews, surveys of current and former extremists, and other empirical analyses of individual pathways to radicalization.

There are several reasons why the internet is such an effective medium for individual radicalization. One reason is the prevalence of virtual echo chambers, which immerse users in homogeneous media environments. The natural human tendency to socialize with like-minded individuals and to seek out information that affirms prior beliefs is reinforced online through algorithmic systems that anticipate user desires and customize the presentation of information. This effect appears to be particularly pronounced in virtual discussions of political issues. For some users, consistent exposure to like-minded virtual communities can discourage consideration of differing views and foster the adoption of more-extreme norms and practices. Users can become cloistered within radical-information environments to a degree that is difficult to replicate in the physical world, either through passive actions—such as the absorption of material presented by algorithms—or through the active search for extreme content or extremist communities. Charismatic influencers can also use online platforms to isolate susceptible users

---

34 Evans and Williams, 2022, pp. 9–12.
35 Evans and Williams, 2022, pp. 11–12.
36 Evans and Williams, 2022, pp. 11–12.
from contrary views and ensure their consistent exposure to the desired message.\textsuperscript{41} Radicalization scholar Peter Neumann has pointed out that these influences can cause people to “acquire a skewed sense of reality so that extremist attitudes and violence are no longer taboos but—rather—are seen as positive and desirable.”\textsuperscript{42}

In these often anonymous and artificial virtual interactions, individuals may have lower inhibitions and an increasing sense of group identification, increasing their trust in others’ descriptions of reality—dynamics that make them susceptible to more-extreme positions.\textsuperscript{43} This promotes less tolerance for differing opinions and groups that hold them, creating a self-reinforcing cycle of commitment to the in-group’s norms and isolation from or rejection of differing viewpoints.\textsuperscript{44} Virtual social networks may shield radicalizing or radicalized individuals from contrary descriptions of reality, inhibiting the 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 out against the perceived threat posed by outsiders.\textsuperscript{45}

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 to both use more-aggressive language and issue direct calls for action.\textsuperscript{46} Research by our colleagues at the RAND Corporation on extremists’ pathways has shown 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{47}


\textsuperscript{46} Koehler, 2014/2015, p. 119.

This is not to say that exposure to a virtual extremist community drives one to offline violence. Social media is only one contributing factor and likely does not substantially alter an individual’s propensity for violence. For some, the ability to find and interact with extremist communities online is an outlet for nonphysical expression. But we can say that the internet likely has increased the number of people exposed to radical ideas, including the far-right grievances that motivated the January 6 assault on the Capitol, and that existing research suggests that internet interactions encourage political polarization and adherence to more-extreme views.\textsuperscript{48}

Also concerning is the fact that internet users still encounter these extreme ideas on any platforms that they use, albeit with varying frequency and ease depending on platform-specific policies and general consumer trends. To differentiate types of social media platforms according to their likelihood of hosting extreme content, RAND developed a framework to identify mainstream platforms (where a small portion of content is composed of inappropriate or extreme speech), fringe platforms (which host a mix of extreme and non-extreme content, and where extremist content is often coded or obscured to disguise its violent and racist underpinnings), and niche platforms (where users readily encounter explicit extreme content).\textsuperscript{49} While our analysis found that fringe platforms may function as transition spaces where extremist views are made more palatable to general audiences, this research underscored that the notion of a separate extremist internet is a myth. Today, almost all platforms host some extremist content. Even though mainstream platforms may maintain and enforce content regulations more aggressively, the sheer volume of content hosted on these platforms—combined with the scale of their user base—means that they possess, in absolute terms, substantially more toxic and hateful material than fringe and niche platforms. Per Twitter’s Transparency Report, 3.8 million tweets were removed in the latter half of 2020 for content violation, over a third of which were marked as hateful or violent. If, as Twitter estimates, 17 percent of these tweets were viewed between 100 and 1,000 times prior to removal and only 6 percent were viewed more than 1,000 times, violating content still received an absolute minimum of 295 million views during this six-month period.\textsuperscript{50} These numbers are available because of Twitter’s efforts at transparency—the situation on other mainstream platforms may be much worse.

Without access to receptive virtual spaces, could far-right extremists set on disrupting U.S. democratic processes have mobilized such a large crowd on the steps of the Capitol? This outcome required the emergence of a mass movement composed of individuals willing to believe online disinformation; the existence of a small, connected group of actors capable of organizing to conduct specifically criminal actions; and the widespread availability of secure, private means to raise revenue, disseminate ideas, coordinate activity, and organize offline events at scale. The internet played a vital role in creating each of these conditions.

There is little evidence to suggest that these dynamics have changed significantly since January 6. Arrests of major leaders, increased public scrutiny, and technology companies’

\textsuperscript{48} Evans and Williams, 2022.
\textsuperscript{49} Williams et al., 2021.
pledges to increase and improve content regulation have forced some elements of the domestic extremist movement to take a tactical pause. But these setbacks appear to be temporary, as extremist movements have leveraged alternative platforms to organize and disseminate propaganda, and they are still able to disseminate the same false and disproven claims of widespread election fraud that inspired the January 6 attack using social media platforms. By portraying themselves as “political prisoners” or “political dissidents,” some extremists have evaded service restrictions and recast their ideas as legitimate, nonviolent political discourse. In the same way that the internet has allowed white supremacist movements to “launder” racist ideas through mainstream forums for public discourse, the national reaction to the events of January 6 has enabled extremists to repackaging their radical ideas and behavior for a wider audience of Americans as legitimate political activity. This has complicated attempts to design and enforce effective content moderation and removal policies and may ensure that the internet remains a receptive domain for extremist movements to gain strength in the future.

---

52 Mark Scott and Rebecca Kern, “The Online World Still Can’t Quit the ‘Big Lie,’” Politico, January 6, 2022.