Testimony

Extremist Use of Online Spaces

Heather J. Williams and Alexandra T. Evans

CT-A1458-1
Testimony submitted to the Select Committee to Investigate the January 6th Attack on the United States Capitol on April 25, 2022.

For more information on this publication, visit www.rand.org/t/CTA1458-1.

Published by the RAND Corporation, Santa Monica, Calif.

www.rand.org

Extremist Use of Online Spaces

Testimony of Heather J. Williams and Alexandra T. Evans[1]
The RAND Corporation[2]

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.

[3] Alexandra T. Evans and Heather J. Williams, *How Extremism Operates Online: A Primer*, Santa Monica, Calif.: RAND Corporation, PE-A1458-2, 2022, https://www.rand.org/pubs/perspectives/PEA1458-2.html.

attack on the U.S. Capitol complex on January 6, 2021.[4] 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 extremists* 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.[5] 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.[6] 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*.

[4] Heather J. Williams, Alexandra T. Evans, Jamie Ryan, Erik E. Mueller, and Bryce Downing, *The Online Extremist Ecosystem: Its Evolution and a Framework for Separating Extreme from Mainstream*, Santa Monica, Calif.: RAND Corporation, PE-A1458-1, 2021, https://www.rand.org/pubs/perspectives/PEA1458-1.html; Evans and Williams, 2022.

[5] Williams et al., 2021.

[6] Office of the Director of National Intelligence, "Domestic Violent Extremism Poses Heightened Threat in 2021," March 1, 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

[7] For a summary of this activity, see Evans and Williams, 2022, p. 4. For additional research, see Anti-Defamation League, *Funding Hate: How White Supremacists Raise Their Money*, New York, 2017, pp. 10–12; Financial Action Task Force, *Ethnically or Racially Motivated Terrorism Financing*, Paris, France, June 2021, pp. 11, 15–16; 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, March 2019, pp. 18–21; and Alex Newhouse, *From Classifieds to Crypto: How White Supremacist Groups Have Embraced Crowdfunding*, Monterey, Calif.: Center on Terrorism, Extremism, and Counterterrorism, Middlebury Institute of International Studies at Monterey, 2019. Despite a growing effort by technology companies to implement new terms of service, analysis of prominent platforms, including PayPal, Squarespace, and Stripe, has found that white supremacists, anti-government militias, and other extremist groups have retained access to these services (Institute for Strategic Dialogue and Global Disinformation Index, *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*, London, United Kingdom, October 27, 2020).

[8] Evans and Williams, 2022, pp. 5–6.

[9] Daniel Koehler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, No. 1, Winter 2014/2015.

[10] Pete Simi and Robert Futrell, "Cyberculture and the Endurance of White Power Activism," *Journal of Political and Military Sociology*, Vol. 34, No. 1, Summer 2006; Pete Simi and Robert Futrell, *American Swastika: Inside the White Power Movement's Hidden Spaces of Hate*, Lanham, Md.: Rowman & Littlefield, 2010.

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-

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

[12] Stephane J. Baele, Lewys Brace, and Travis G. Coan, "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism*, 2020, pp. 6, 15; W. Chris Hale, "Extremism on the World Wide Web: A Research Review," *Criminal Justice Studies*, Vol. 25, No. 4, 2012, pp. 347, 349–350.

[13] Evans and Williams, 2022, pp. 6–7, 11–12.

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

[15] Jamie Bartlett, "From Hope to Hate: How the Early Internet Fed the Far Right," *The Guardian*, August 31, 2017; Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America*, Cambridge, Mass.: Harvard University Press, 2018, pp. 213, 237.

[16] Mattias Ekman, "The Dark Side of Online Activism: Swedish Right-Wing Extremist Video Activism on YouTube," *MedieKultur: Journal of Media and Communication Research*, Vol. 30, No. 56, 2014; Robin Pomeroy, "Facebook Pulls Italian Neo-Nazi Pages After Outcry," Reuters, November 14, 2008; Abby Rogers, "These Pictures Show That Wade Michael Page Was a Devoted Neo-Nazi," *Insider*, August 7, 2012; Kevin Roose, "The Alt-Right

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

Created a Parallel Internet. It's an Unholy Mess," *New York Times*, December 11, 2017; "Sikh Temple Shooter Said to Be White Supremacist," *Columbus Dispatch*, August 6, 2012.

[17] "Norway Suspect Calls Massacre 'Marketing Method,'" Associated Press, July 24, 2011; Southern Poverty Law Center, "White Homicide Worldwide," April 1, 2014.

[18] European Commission, "Code of Conduct on Countering Illegal Hate Speech Online," May 31, 2016.

[19] Eshwar Chandrasekharan, Shagun Jhaver, Amy Bruckman, and Eric Gilbert, "Quarantined! Examining the Effects of a Community-Wide Moderation Intervention on Reddit," arXiv preprint, arXiv:2009.11483, 2020; Adi Robertson, "Reddit Bans 'Fat People Hate' and Other Subreddits Under New Harassment Rules," *The Verge*, June 10, 2015; Adi Robertson, "Welcome to Voat: Reddit Killer, Troll Haven, and the Strange Face of Internet Free Speech," *The Verge*, July 10, 2015.

[20] Seth G. Jones, James Dobbins, Daniel Byman, Christopher S. Chivvis, Ben Connable, Jeffrey Martini, Eric Robinson, Nathan Chandler, *Rolling Back the Islamic State*, Santa Monica, Calif.: RAND Corporation, RR-1912, 2017, pp. 175–176, 181–185, https://www.rand.org/pubs/research_reports/RR1912.html.

[21] Kent Walker, "Four Steps We're Taking Today to Fight Terrorism Online," Google, June 18, 2017.

focused specifically on Islamist extremists.[22] Far-right extremists, meanwhile, were still using online spaces to organize mass demonstrations, establish small militant cells, and inspire individual acts of violence.[23]

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."[24] 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.[25] 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.[26]

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.[27] 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.[28] 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,

[22] Gardiner Harris and Cecilia Kang, "Obama Shifts Online Strategy on ISIS," *New York Times*, January 8, 2016; U.S. Senate, *ISIS Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media: Hearing Before the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs*, Washington, D.C.: U.S. Government Publishing Office, 2016.

[23] Luke O'Brien, "The Making of an American Nazi," *The Atlantic*, December 2017; Soufan Center, *The Atomwaffen Division: The Evolution of the White Supremacy Threat*, New York, August 2020.

[24] Twitter, "Enforcing New Rules to Reduce Hateful Conduct and Abusive Behavior," blog post, December 18, 2017, https://blog.twitter.com/en_us/topics/company/2017/safetypoliciesdec2017.

[25] Heather Kelly, "Hate Groups on Facebook: Why Some Get to Stay," CNN, August 17, 2017; Casey Newton, "Discord Bans Servers That Promote Nazi Ideology," *The Verge*, August 14, 2017.

[26] Colin Lecher, "Squarespace Says It's Removing 'a Group of Sites' as Internet Cracks Down on Hate Speech," *The Verge*, August 16, 2017; Ryan Mac and Blake Montgomery, "Apple Pay Is Cutting Off White Supremacists," BuzzFeed News, last updated August 17, 2017.

[27] Maura Conway, "Routing the Extreme Right: Challenges for Social Media Platforms," *RUSI Journal*, Vol. 165, No. 1, January 2020.

[28] J. M. Berger, "The Dangerous Spread of Extremist Manifestos," *The Atlantic*, February 26, 2019; Robert O'Harrow, Jr., Andrew Ba Tran, and Derek Hawkins, "The Rise of Domestic Extremism in America," *Washington Post*, April 12, 2021.

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.

[29] Adi Robertson, "Gab Is Back Online After Being Banned by GoDaddy, PayPal, and More," *The Verge*, November 5, 2018.

[30] Evans and Williams, 2022, pp. 8–13.

[31] Ken Dilanian and Ben Collins, "There Are Hundreds of Posts About Plans to Attack the Capitol. Why Hasn't This Evidence Been Used in Court?" NBC News, April 20, 2021; Sheera Frenkel, "The Storming of Capitol Hill Was Organized on Social Media," *New York Times*, January 6, 2021; Craig Timberg and Drew Harwell, "Pro-Trump Forums Erupt with Violent Threats Ahead of Wednesday's Rally Against the 2020 Election," *Washington Post*, January 5, 2021.

[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.[34] 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.[35] 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.[36]

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.[37] This effect appears to be particularly pronounced in virtual discussions of political issues.[38] 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.[39] 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.[40] 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.

[37] James N. Cohen, "Exploring Echo-Systems: How Algorithms Shape Immersive Media Environments," *Journal of Media Literacy Education*, Vol. 10, No. 2, 2018; M. D. Conover, J. Ratkiewicz, M. Francisco, B. Gonçalves, A. Flammini, and F. Menczer, "Political Polarization on Twitter," *Proceedings of the 5th International AAAI Conference on Weblogs and Social Media*, Vol. 5, No. 1, 2021; Michael A. DeVito, "From Editors to Algorithms: A Values-Based Approach to Understanding Story Selection in the Facebook News Feed," *Digital Journalism*, Vol. 5, No. 6, 2017; Ivan Dylko, Igor Dolgov, William Hoffman, Nicholas Eckhart, Maria Molina, and Omar Aaziz, "Impact of Customizability Technology on Political Polarization," *Journal of Information Technology & Politics*, Vol. 15, No. 1, 2018; R. Kelly Garrett, "Echo Chambers Online? Politically Motivated Selective Exposure Among Internet News Users," *Journal of Computer-Mediated Communication*, Vol. 14, No. 2, 2009; Matthew J. Kushin and Kelin Kitchener, "Getting Political on Social Network Sites: Exploring Online Political Discourse on Facebook," *First Monday*, Vol. 14, No. 11, November 2009.

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

[39] Natalie Jomini Stroud, "Polarization and Partisan Selective Exposure," *Journal of Communication*, Vol. 60, No. 3, 2010; Magdalena Wojcieszak, "'Don't Talk to Me': Effects of Ideologically Homogeneous Online Groups and Politically Dissimilar Offline Ties on Extremism," *New Media & Society*, Vol. 12, No. 4, 2010.

[40] Maura Conway, Ryan Scrivens, and Logan Macnair, *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends*, The Hague, Netherlands: International Centre for Counter-Terrorism, October 2019; Gaudette, Scrivens, and Venkatesh, 2020, p. 13.

from contrary views and ensure their consistent exposure to the desired message.[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."[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.[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.[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.[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.[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."[47]

[41] For studies exploring how the internet enables extremist groups to control or influence the information presented to their members, see Joseph A. Carter, Shiraz Maher, and Peter R. Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, London, United Kingdom: International Centre for the Study of Radicalisation and Political Violence, 2014; and Jytte Klausen, "Tweeting the *Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, Vol. 38, No. 1, 2015.

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

[43] For an early study describing this phenomenon, see Russell Spears, Martin Lea, and Stephen Lee, "De-Individuation and Group Polarization in Computer-Mediated Communication," *British Journal of Social Psychology*, Vol. 29, No. 2, June 1990. See also Koehler, 2014/2015, p. 118; and John Suler, "The Online Disinhibition Effect," *International Journal of Applied Psychoanalytic Studies*, Vol. 2, No. 2, June 2005.

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

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

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

[47] Ryan Andrew Brown, Todd C. Helmus, Rajeev Ramchand, Alina I. Palimaru, Sarah Weilant, Ashley L. Rhoades, and Liisa Hiatt, *Violent Extremism in America: Interviews with Former Extremists and Their Families on Radicalization and Deradicalization*, Santa Monica, Calif.: RAND Corporation, RR-A1071-1, 2021, p. 87, https://www.rand.org/pubs/research_reports/RRA1071-1.html.

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.[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).[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.[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'

[48] Evans and Williams, 2022.

[49] Williams et al., 2021.

[50] Twitter, Inc., *Twitter Transparency Report: Rules Enforcement, Jul–Dec 2020*, July 14, 2021.

pledges to increase and improve content regulation have forced some elements of the domestic extremist movement to take a tactical pause.[51] 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.[52] By portraying themselves as "political prisoners" or "political dissidents," some extremists have evaded service restrictions and recast their ideas as legitimate, nonviolent political discourse.[53] In the same way that the internet has allowed white supremacist movements to "launder" racist ideas through mainstream forums for public discourse,[54] the national reaction to the events of January 6 has enabled extremists to repackage 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.

[51] Jared Holt, *After the Insurrection: How Domestic Extremists Adapted and Evolved After the January 6 US Capitol Attack*, Washington, D.C.: Atlantic Council, January 2022.

[52] Mark Scott and Rebecca Kern, "The Online World Still Can't Quit the 'Big Lie,'" *Politico*, January 6, 2022.

[53] Ed Pilkington, "Capitol Attack Insurrectionists Flock to Fundraising Websites to Raise Defense Funds," *The Guardian*, December 17, 2021.

[54] Adam Klein, "Slipping Racism into the Mainstream: A Theory of Information Laundering," *Communication Theory*, Vol. 22, No. 4, November 2012.