NATIONAL INSTITUTE OF JUSTICE

THE ROLE OF THE INTERNET AND SOCIAL MEDIA ON RADICALIZATION

What Research Sponsored by the National Institute of Justice Tells Us

Kateira Aryaeinejad and Thomas Leo Scherer, Ph.D.

APRIL 2024

NIJ.OJP.GOV | NATIONAL INSTITUTE OF JUSTICE

ADVANCING JUSTICE THROUGH SCIENCE

U.S. Department of Justice
Office of Justice Programs

810 Seventh St. N.W.
Washington, DC 20531

Nancy La Vigne, Ph.D.
Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
Advancing Justice Through Science
NIJ.ojp.gov

Office of Justice Programs
Building Solutions • Supporting Communities • Advancing Justice
OJP.gov

Executive Summary

The National Institute of Justice's (NIJ) Domestic Radicalization to Terrorism program has funded research on different facets of domestic radicalization to terrorism within the United States since 2012. Although the focus of NIJ-sponsored research on this phenomenon has varied, an aspect common among funded projects is the role of social media and the internet in influencing radicalization and violent extremist dynamics. This synthesis paper draws from these studies, exploring the information within them that lends additional insight into how the virtual space may influence radicalization processes in the United States. In doing so, the paper advances a framework for conceptualizing the different ways in which the internet may be used or provide potential pathways to (and away from) networks and content that may influence individual radicalization trajectories.

It was outside the scope of this synthesis to review internet-related findings from the entirety of the NIJ-sponsored research portfolio, of which there are many. Rather, this paper focuses on studies with published results that specifically focused on the role of the online space, synthesizing findings based on four main criteria: online exploitation, online engagement, online risk, and online mitigation. Importantly, while the NIJ-sponsored studies detailed in this paper are not scientifically comparable — drawing from a variety of populations, online areas of focus, and periods of time — overall, they provide information useful in informing future policy, programs, and studies focused on radicalization and terrorism in the online space.

Synthesized findings from the body of research examined suggest that, much like other dynamics and factors, the role of the internet in radicalization processes is complex and not necessarily clear cut. Although findings suggest that the internet does play a role in facilitating information sharing, networking, and engagement with potentially hateful and violent extremist materials, the extent to which social media and the internet function as a direct and singular cause of radicalization is unclear. Indeed, it may vary based on (and even within similar) individual characteristics, backgrounds, and ideological influences. For example, one study examined differences in the types and prevalence of explicitly ideological material within online far-right forums. Another examining female trajectories to radicalization and their use of the internet also found similar variation in the extent of online engagement among different types of individuals categorized as low, medium, or high based on the nature of their violent extremist activities.

Moving forward, while there is a broad need for additional understanding of the role of the internet and social media in radicalization, current findings also provide important insight into areas of research worth building on and gaps to fill in. Further research is especially

needed in understanding how the risk of radicalization varies across different online materials. Likewise, additional research is needed on how extremists tailor their messages and methods to try to increase the effectiveness of their recruitment and radicalization efforts.

The findings also illuminate how policymakers and practitioners seeking to prevent and reverse radicalization must tailor their engagement across different platforms just as recruiters do. At the same time, they must also consider how internet and social media use is just one part of a larger radicalization strategy that has to be addressed holistically. Similarly, efforts to address violent extremism online may overlap with other violence reduction efforts. Where that is the case, coordination and prioritization become necessary and beneficial for all efforts.

Introduction

The National Institute of Justice's (NIJ) Domestic Radicalization to Terrorism program began funding research about radicalization to terrorism in the United States in 2012. These studies have since yielded valuable findings for policy and practice.[1] As part of an ongoing effort to synthesize findings derived from this body of research as they relate to terrorism prevention efforts, this paper examines several NIJ-funded projects, highlighting insights from research on the role of the internet and social media in domestic radicalization.[2]

Research on the role of online spaces and social media in facilitating or motivating terrorism and radicalization has grown exponentially over the past decades.[3] As online technologies and internet platforms become increasingly integrated into day-to-day life, the impact and role of terrorism, violent extremism, and radicalization in online spaces remain cause for concern. Previous research illuminates the varied and evolving role the internet may play in facilitating violent extremist and terrorist activities and recruitment.[4] From the sharing of violent extremist propaganda and the posting of online manifestos[5] to the livestreaming of violent extremist attacks, the role of the internet in radicalizing individuals to violence and facilitating violent attacks remains a pressing policy and research issue, with varied recommendations on how to best address it.[6] Findings from NIJ-sponsored research over the past two decades add important insight and nuance to our collective understanding of the role that the internet and online social media can play in fostering or facilitating radicalization to violent extremism and terrorism within the United States. This paper details those findings, which focus not only on understanding how online spaces can influence radicalization outcomes, but also on how those outcomes may be impacted by individual online behaviors and activities.

The paper begins by framing the different roles the internet and online dynamics may have in influencing radicalization to terrorism or violent extremism. It then provides an overview of NIJ-sponsored research focusing specifically on the role of the internet and social media in facilitating or mitigating individual radicalization processes. Although many NIJ-sponsored studies address this phenomenon, in the interest of the topic at hand, only those focused specifically on online and social media networks are discussed in detail. Following

this overview of online-specific projects, the paper details synthesized findings from the projects before discussing important caveats, remaining areas for research, and implications for policy and practice.

Although this paper is focused on the role of the internet and social media in influencing radicalization, an additional NIJ research synthesis paper also addresses the topic of both online and offline social networks and their impact on radicalization outcomes.[7] Findings from this additional paper are cited, where relevant, as they pertain to the role of online social networks in influencing or mitigating radicalization processes.

Understanding the Role of Social Media and the Internet in Radicalization: Exploitation, Engagement, Risk, and Mitigation

Awareness of the potential impact of virtual connections and platforms in housing violent extremist content and connecting individuals who support violent extremist ideologies and movements is growing. Alongside this awareness, attention to the role of social media and online spaces as potential drivers of radicalization has increased. Much of this attention has been focused on the so-called Islamic State's use of the internet and social media to spread propaganda and recruit individuals worldwide to travel to Iraq and Syria.[8] However, in the wake of recent events, focus on far-right and white supremacist extremists' use of the internet to livestream attacks, connect, and share information and ideological materials has also increased.[9]

The use of online platforms and social media by violent extremist and terrorist actors is not necessarily new.[10] Still, understanding how the internet and social media influence radicalization trajectories requires understanding which virtual spaces are used, how those spaces are used, and by whom. For this paper, online activities related to violent extremism and radicalization are conceptualized as falling into four main categories: exploitation, engagement, risk, and mitigation.

Exploitation is conceived in this paper as how individuals and groups use online spaces to spread extremist ideologies and further their goals. Violent extremist groups and terrorist actors have a long history of online engagement and social media usage. From spreading ideology and propaganda to fundraising, sharing tactics, and recruiting individuals, violent extremist and terrorist actors exploit online platforms and forums with varied

impacts and effects.[11] Understanding the strategies and tactics of these actors, the impact of their methods, and how their online activities feed into their strategic goals is of great importance in crafting effective policy and interventions to address them.

Closely related to exploitation, **engagement** is conceptualized in this paper as how individuals engage with others and consume violent extremist materials and content online — including how that content and material can, in turn, affect radicalization outcomes and trajectories. Engagement activities can include seeking validation for violent extremist beliefs and sentiments, consuming violent extremist propaganda and content, communicating intent to take violent action (also referred to as "leakage"),[12] and seeking out like-minded individuals through online platforms. Understanding engagement and the factors that impact it (both positively and negatively) sheds light on how violent extremist exploitation of online spaces — and the connections made within them — may impact radicalization trajectories. It is important to note, however, that individuals who encounter or engage with violent extremist content online do not necessarily radicalize, as suggested by findings from some of the NIJ-sponsored studies discussed herein. This underscores the importance of research focusing on not only whether or how individuals engage with violent extremist content and communities online, but the impact that content and those communities have on those engaging with them.

Risk is characterized in this paper as how an individual's online behaviors and individual factors may put them at risk of interacting, engaging, or viewing potentially radicalizing or violent extremist content. Efforts to understand risk online can include "upstream factors" — online behaviors and activities that increase the likelihood that an individual encounters, consumes, or engages (either in a benign or malignant fashion) with terrorist and violent extremist content. Though not always directly tied to radicalization to violent extremism, risk provides useful insight into individual and gateway factors that may increase the likelihood that an individual is exposed to violent extremist actors and content, and insight into the potentially radicalizing factors such engagement can bring. Much like consumption, "risk" as defined here may contribute to radicalization trajectories but cannot be analyzed effectively without considering other individual factors. Rather, research on the subject provides essential insight into behaviors and online pathways that may make it more likely that an individual will be exposed to violent extremist materials and actors online.

Finally, **mitigation** refers to protective factors — including behaviors, policies, and characteristics. These factors may decrease the likelihood of an individual engaging with potentially radicalizing content and individuals online and on social media. In addition, these factors may divert or intervene when an individual is on a pathway to radicalization. Policy and practitioner responses ranging from counternarrative communications and online off-ramping initiatives to de-platforming and counter dis/misinformation efforts may be used as mitigating forces, as can individual online reporting behaviors and activities.

Of course, each of these four categories — exploitation, engagement, risk, and mitigation — can overlap in online spaces. For example, those consuming violent extremist content can also be those exploiting online systems to spread violent extremist ideologies. The nature of the individual and the point in time in which they experience exploitation, engagement, risk, or mitigation may also play a major role in the radicalization process.[13] NIJ-sponsored research focusing on the role of the internet and social media illuminates findings related to each of these categories, with important implications for policy and practice.[14]

NIJ-Sponsored Research on the Role of the Internet and Social Media in Radicalization Processes

This section summarizes recent NIJ-sponsored research on the role of the internet and social media in domestic radicalization processes. Exhibit 1 lists research on the influence of online engagement and interaction in radicalization processes. Although the research varies in focus based on temporal, ideological, online, and point-of-influence (or stages of impact on radicalization) dynamics, collectively, the findings offer important areas of consideration and opportunities for further exploration for policy and research.

Exhibit 1: Overview of Select NIJ-Sponsored Research on the Internet and Social Media

Year	Grant No.	Project Title	Primary Grantee	Brief Project Summary
2014 - 2021	2014-ZA-BX-0004	An Assessment of Extremist Groups Use of Web Forums, Social Media, and Technology to Enculturate and Radicalize Individuals to Violence	Michigan State University	The Michigan State University researchers collected and analyzed postings from far-right online forums to understand the role of computer communication in violence promotion, enculturation, and radicalization.[1]
2014 - 2021	2014-ZA-BX-0014	Radicalization on the Internet: Virtual Extremism in the U.S. from 2012-2017	Arkansas State University	The Arkansas State University team compiled information on hate group activity online and surveyed 3,000 Americans on their internet habits and their exposure and reaction to hate groups' online material.[2]
2015 - 2019	2015-ZA-BX-0004	Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence	University of Maryland	As a part of their larger research efforts, the University of Maryland team collected social media data on individuals who engaged in violent and nonviolent hate crimes or criminal activities in furtherance of ideological goals to understand and compare radicalization processes.[3]

Exhibit 1: Overview of Select NIJ-Sponsored Research on the Internet and Social Media (continued)

Year	Grant No.	Project Title	Primary Grantee	Brief Project Summary
2016 - 2020	2016-ZA-BX-K002	Social Media as a Platform for Crafting Gender-Specific Interventions for the Domestic Radicalization of Women	The Rector and Visitors of the University of Virginia	As part of a larger research effort, researchers at the University of Virginia examined the role of social media in recruiting and radicalizing women by coding risk characteristics of 300 women associated with violent extremism, including online engagement.[4]
2018 - ongoing	2018-ZA-CX-0002	Operation250: An Evaluation of a Primary Prevention Campaign focused on Online Safety and Risk Assessment	University of Massachusetts-Lowell	The University of Massachusetts-Lowell team carried out a project involving a formative and summative randomized controlled trial evaluation with nonprofit Operation250 to test the effects of their internet safety counterterrorism programming.[5]

1. Thomas J. Holt, Steve Chermak, and Joshua D. Freilich, "Assessment of Extremist Groups Use of Web Forums, Social Media, and Technology to Enculturate and Radicalize Individuals to Violence," Final report to the National Institute of Justice, award number 2014-ZA-BX-0004, January 2021, NCJ 256038, https://www.ojp.gov/pdffiles1/nij/grants/256038.pdf.
2. Matthew Costello et al., "Radicalization on the Internet: Virtual Extremism in the U.S. from 2012-2017," Final report to the National Institute of Justice, award number 2014-ZA-BX-0014, January 2021, NCJ 256036, https://www.ojp.gov/pdffiles1/nij/grants/256036.pdf.
3. Gary LaFree, "Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence," Final report to the National Institute of Justice, award number 2015-ZA-BX-0004, January 2021, NCJ 256024, https://www.ojp.gov/pdffiles1/nij/grants/256024.pdf.
4. Janet I. Warren et al., "The Creation of Muhajirat in America: Social Media as a Platform for Crafting Gender-Specific Interventions for the Domestic Radicalization of Women," Final report to the National Institute of Justice, award number 2016-ZA-BX-K001, September 2020, NCJ 255237, https://www.ojp.gov/pdffiles1/nij/grants/255237.pdf.
5. National Institute of Justice funding award description, "Operation250: An Evaluation of a Primary Prevention Campaign focused on Online Safety and Risk Assessment," at the University of Massachusetts, award number 2018-ZA-CX-0002, https://nij.ojp.gov/funding/awards/2018-za-cx-0002.

An Assessment of Extremist Groups' Use of Web Forums, Social Media, and Technology To Enculturate and Radicalize Individuals to Violence

In their NIJ-sponsored research,[15] a team at Michigan State University examined seven far-right-aligned[16] web forums, as well as threads from subforums within them, to investigate the nature, networks, extent, and means by which online communications and ideological expressions manifest in shared online spaces to produce radicalization outcomes and "enculturation" in violent extremist ideologies. Five of the seven forums were associated with far-right-aligned groups, and the other two were identified as being unaffiliated with any specific far-right organized group.

Using data from 18,120 posts across forums spanning the years 2001-2016,[17] the researchers sought to answer five main questions surrounding far-right postings online, related to (1) how ideologies are expressed, (2) changes in communication over time among those engaged in online far-right communities, (3) discussions of technology use and computer security, (4) social network structures, and (5) changes in communication coinciding with or preceding violent acts and events.[18] Additional outputs from the project also included in-depth analysis of a women-only Ku Klux Klan forum.[19]

Overall, the findings yielded valuable insights into the use of digital communications among far-right-aligned individuals operating within the online forums from which data were gathered. Notably, the results suggested that the far right is not monolithic online; that is to say, the far-right community online encompasses a diversity of perspectives and ideological leanings. Indeed, variations in posting behaviors and ideological content were

observed throughout the forums studied, including notably between forums that were affiliated with real-world far-right groups versus those without specific group affiliations.[20] Findings also hinted at the possible impact of online engagement, with evidence suggesting that not only did individuals within the forums become somewhat more ideological over time, but also that connections within and reinforcement across forums were associated with a greater likelihood of espousing radical views as time progressed.[21] However, additional findings left open the possibility that individuals already harboring radical beliefs may use forums not to engage with others, but to seek additional information.[22] This not only highlights how individuals may use the internet and social media for different purposes and at different stages of the radicalization process; it also, as the authors point out, calls into question how the internet influences radicalization trajectories vis-a-vis other influences, including those in the offline space.

Additional insights from the research revealed that far-right online forums tended to be "relatively insular," operating primarily as echo chambers, but without much efficiency in spreading new information or strong evidence of technological sophistication.[23] Some evidence also suggested that far-right online activities and sentiments may be more impacted by offline events involving perceived enemies or significant changes rather than offline events involving far-right actors.[24] Ultimately, based on the findings, the research team suggested the need for further research and more targeted interventions focused on online far-right reactions to specific offline events and critical differences in the ideological leanings of different far-right actors and online forums. The researchers also called for further research as to the impact that online engagement has on offline activities.

Radicalization on the Internet: Virtual Extremism in the United States From 2012 to 2017

To understand how people are exposed to and react to online extremism, the research team at Arkansas State University surveyed 3,000 Americans. The survey took place over three years and targeted a nationally representative group of 15- to 36-year-olds.[25] Using these data, the research team has published numerous papers on the relationship between different factors.

The survey asked respondents how often they saw material online that expressed negative views toward a group, which was used as a proxy for their exposure to online hate material.[26] Among 15- to 24-year-olds, this measure was positively correlated with a respondent's dissatisfaction with the current direction of the United States and mistrust of politicians. It was also correlated with their time online and reported usage of Snapchat, YouTube, and Reddit, but not with their reported usage of Facebook, Twitter, or Google+. Interestingly, the researchers found Instagram to be a platform where users were "significantly less likely" to encounter hateful materials frequently.[27] Additional publications from the project examined online exposure to negative views focused on race, sex, nationality, religion, and political views, and exposure to negative views that advocated violence.[28] The team also looked at who was targeted by negative material based on their internet behavior[29] or their sexual orientation,[30] and which types of conflict management styles are correlated with a higher risk of online crime.[31] In addition, the respondents answered how frequently they defended a group or told someone to stop when they encounter offensive material, allowing the team to study which types of bystanders are more likely to intervene.[32] The researchers also used the survey to understand the creation and dispersion of negative materials. One analysis looked at when respondents perpetuated online hate, as measured by how often they engaged in

behavior they found mean or approved of mean materials.[33] Higher frequencies were reported by males, people with low levels of self-control, and those who had been a target of online hate or online crime. Also, respondents who interacted with close friends online, were close to an online community, or frequently saw hate online were more likely to join in hateful behavior. Other work looked at associations among those who produced negative online material.[34]

Social Learning and Social Control in Offline and Online Pathways to Hate and Extremist Violence

University of Maryland researchers compared the trajectories of violent extremists and individuals who committed hate crimes using three types of data, both offline and online. First, they merged the United States Extremist Crime Database and Profiles of Individual Radicalization in the United States and linked 454 overlapping individuals.[35] Second, they created 38 case studies of individuals and compared their radicalization processes in several articles (including one discussed in an earlier report in this series focused on social networks).[36] Finally, using terms from the case studies, the team searched for and recorded the social accounts of 52 individuals, including 29 far-right actors, 21 Islamists, and two individuals on the far left.[37]

The case studies conducted for this project show how the internet can be an important source of social connection and communication in relation to radicalization.[38] For example, in an article comparing four cases, the internet was thought to play a key role in the radicalization of two far-right extremists. For one individual, the internet appeared to initiate their shift towards anti-government extremism by providing material and videos promoting conspiracy theories; for the other, the internet solidified their growing extremism.[39] The search for social media accounts proved difficult. The research team found nine Facebook accounts (17%), one Google+ account (2%), three YouTube accounts (6%), three Twitter accounts (6%), and three personal websites (6%). They found signs of accounts on Friendster, Snapchat, and Instagram and other platforms but were not able to verify all possible accounts on those platforms. Notably, the researchers make explicit that Instagram use was deemed relatively uncommon. Similar to the case study comparison described above, the Facebook accounts suggested higher activity by far-right individuals, with seven accounts found versus only two for Islamists.[40]

Social Media as a Platform for Crafting Gender-Specific Interventions for the Domestic Radicalization of Women

The University of Virginia research team wanted to understand and respond to social media campaigns by groups like the Islamic State of Iraq and the Levant designed to recruit and persuade women.[41] Following the situational action theory of crime, the researchers formulated a moral-situational action model of extremist violence that considers three dimensions. *Propensity* is an individual's values and self-regulatory capabilities that determine their susceptibility to radicalizing materials. *Mobilization* is an individual's interaction with their social setting and their activity patterns (including cyber interaction).

Action and capacity-building is the perpetration of extremist violence and the actions that precede and support that violent action.[42] The researchers applied this model to a sample of 300 women previously involved with violent extremism. The research team gathered background sources and social media for each subject and then coded each case for 496 variables. The subjects were assigned risk categories based on their riskiest action. Their category was *high* if they were involved in direct action (43%), *medium* if they were only involved as plotters, recruiters, or material disseminators (50.6%), or *low* if they were only travelers, agents of state-building, or supporters (6.3%).

The researchers found that 52% of the medium-risk category had virtual communities, versus only 15.5% of the high-risk and 10.5% of the low-risk categories. For the 137 subjects with cyber interactions, the medium-risk category had the highest percentage that used cyberspace to consume radical content (38.8%), share radical content (41.4%), create radical content (21.1%), endorse attacks (11.8%), post about committing attacks (3.3%), and actively recruit (24.3%). Subjects in the low-risk category were the most likely to be actively recruited through cyber interactions (26.3%).[43]

For each dimension, regressing whether someone was high risk or medium/low risk on their demographics and dimension-specific propensity variables showed that some propensity factors were related to their risk category. A regression model that included all of the significant variables across dimensions had an in-sample accuracy of 76%. No out-of-sample testing was reported.[44]

Operation250: An Evaluation of a Primary Prevention Campaign Focused on Online Safety and Risk Assessment

Operation250 is a nonprofit organization that works on online safety from hate and extremism. The organization was started by students around the Peer 2 Peer Challenging Extremism Initiative and was part of an evaluation in an earlier NIJ-sponsored grant.[45] Following that research, a University of Massachusetts-Lowell team partnered with Operation250 to understand the effects of Operation250's workshops and programs.

The research is ongoing, but the project already has several preliminary findings. First, Operation250 programs were highly malleable and inconsistent, as Operation250 tailored the programs for each school. Although logical, this inconsistency was rooted more deeply in uncertainty regarding the organization's focus. The lack of consistent programs across settings makes it difficult to build a body of research on a program's effects in different contexts.[46] Second, measuring success beyond engagement and retention (i.e., outputs) to include behavior and knowledge (i.e., outcomes) is difficult, especially within practical constraints like the limited attention span of children for questionnaires. The University of Massachusetts-Lowell team reported that developing deeper measures was difficult, but the new scales developed from this research have led to intriguing findings. After one program, students reported higher levels of online disinhibition, which is not the desired effect. One possible explanation is that the program promotes greater self-reflection and awareness among participants, who subsequently realize they are more disinhibited than they previously understood. Further research is clearly needed — but with better measures, there is a path forward.[47]

Out of this project, the University of Massachusetts-Lowell team also wrote about the criticisms that work in countering violent extremism (CVE) sometimes receives. Drawing from the public health literature, they proposed four criteria for determining whether a CVE project is ethically justified.[48] First, how much does the program impinge on civil liberties? Second, is the program proportional in terms of minimizing harm and achieving its goals? Third, is the program the least infringing policy that can achieve the goal? Fourth, does the program have widespread support? Given the frequent lack of careful, ethical consideration in CVE programs, these criteria offer a helpful guide for practitioners.

Synthesized Findings: The Role of Online Exploitation, Engagement, Risk, and Mitigation

Collectively, findings from NIJ-sponsored research on the role of the internet and social media in radicalization suggest that although online dynamics may play some part in radicalizing individuals to terrorism in the United States, that role can vary significantly depending on several factors related to online exploitation, engagement, risk, and mitigation.

Before discussing collective findings, however, it should be noted that certain caveats may limit the ability to look across projects and glean generalized findings. For one, the projects listed above differed significantly in the samples from which their findings and conclusions were drawn. Data for each project varied in when they were gathered, the methods used, the inclusion and exclusion criteria selected, and the populations from which they were drawn — ranging from individuals who had already engaged in acts of violent extremism and hate-related offenses, to youth who simply use the internet and interact with others virtually, to individuals with different ideological leanings who interact online. Although this range is not necessarily problematic in itself — indeed, it provides a somewhat all-encompassing snapshot of different elements to consider — it does impose certain limitations on our ability to compare project findings and synthesize them in a scientific manner.

Although findings derived from data from past time periods regarding online and social media use are certainly valuable, they may not provide the most up-to-date or accurate picture of the impact of the internet and social media on radicalization dynamics today. This is particularly so given the rapid pace at which online platforms and usership have evolved over the past decade and continue to evolve. This, however, does not negate the value of the research or the findings discussed within this report. Although time-bound, this information can present us with important snapshots and insights into how the internet was used in the past. Moreover, based on the varied timelines of the NIJ-sponsored research

discussed in this report, the findings provide insight into how trends potentially related to radicalization and the use of the internet may vary across different time periods, which may be useful in considering and analyzing present-day online dynamics.

Additionally, a crucial caveat when considering any research online is the extent to which difficulties associated with measuring online behaviors and identifying online violent extremist content and individuals impact research findings. Issues associated with respondent bias in survey data focused on online behaviors, as noted by some of the NIJ-sponsored research teams,[49] may have impacted data validity. Furthermore, issues associated with anonymity, identifying violent extremists online, isolating the impact of online versus offline dynamics and experiences, and determining the intent behind online postings are pervasive in studying the role of the internet and social networks in radicalization processes. The possibility that the content and actors examined in research on the internet and radicalization may not be violent extremist in nature (or carry the intent to radicalize or spread violent extremist content) should be kept in mind by readers. So too should definitions used within the research and how the research has identified "hate content," "violent extremists," and "terrorists" in otherwise largely anonymous or easily de-identified online spaces.

With these caveats in mind, the synthesized findings below should not be seen as broadly representative nor generalizable due to the diverse nature of the methods, data, definitions, and focuses of the projects examined here. Collectively, however, these findings provide insight into potential areas where the internet and social media might impact radicalization trajectories in the United States, by possibly fostering increased radicalization and preventing or addressing radicalization before it leads to violence. Taken as a whole, the findings highlight important gaps and avenues for further research. To illuminate these insights and areas for further exploration, we turn back to the framework laid out in the opening sections of this paper to structure our discussion and examine what findings from NIJ-sponsored research can tell us about how the following may influence radicalization outcomes:

- Violent extremist **exploitation** of virtual spaces

- Individual and collective **engagement** with violent extremist content or with peers virtually and on social media

- **Risk** factors, or elements increasing the likelihood of interaction with violent extremism online

We reserve discussion of factors that may **mitigate** the role played by online risk, exploitation, and engagement for a later section on implications for policy and practice.

Online Exploitation and Engagement's Complicated Relationship With Radicalization

Regarding violent extremist and terrorist exploitation of the internet and social media and the role that engagement with online violent extremist communities and content plays in domestic radicalization processes, NIJ-sponsored research raises more questions than it can currently answer. This is not to suggest that the research should be disregarded, but rather, to serve as a reminder that radicalization processes vary. Potential for radicalization in the online space is no different.

A prime example is the University of Virginia's finding that 52% of women in the medium-risk category had virtual communities, versus only 15.5% in the high-risk category and 10.5% in the low-risk category. This finding is counterintuitive if we assume risk level rises in parallel with connecting to virtual communities. However, the fact that those in the medium-risk category were categorized as plotters, recruiters, or material disseminators, as suggested by the researchers, also raises the question of how internet usage by violent extremist-aligned individuals differs based on the goals of the individual using it.[50] Although we can imagine other explanations related to the timing of the development of the internet and different profiles of high-, medium-, and low-risk individuals, further research is needed to understand these phenomena.

In addition, divergences within the findings of the Michigan State University team's study of far-right online forums further complicate our efforts to understand the role of the internet in facilitating radicalization. As noted by the study's authors, while some evidence suggested that engagement in these online spaces may correlate with more radical or ideological beliefs (at least outwardly) over time, some individuals who showed little communication with others in these online communities were found to be more likely to be ideologically expressive.[51] Furthermore, findings from this study suggested distinct differences in ideological expression between forums that were affiliated with an offline group versus those that were not.[52] This, as the researchers suggest, supports other studies that highlight the diversity in individual radicalization processes.[53] Variations such as these are worthy of further study, and they highlight questions of *who* may be more susceptible to radicalization online and *why*.

Indeed, findings from NIJ-sponsored research suggest that virtual engagement and exploitation may be both a cause and a consequence of radicalization. In their study of far-right online forums, the research team at Michigan State University found evidence supportive of the notion that "involvement in ideological communities may play a key role in radicalization," given that individuals in forums with greater interaction with and reinforcement from others became somewhat more ideological over time.[54] However, the team also noted that some individuals who did not engage with others in the forums were more likely to be "ideologically expressive."[55] This, as the team alludes to, raises the question "Do individuals radicalize because of online connections, or are the individuals drawn to online forums already radicalized?" It also underlines the importance of considering online radicalization processes outside of a binary lens (either the internet radicalizes an individual or an individual uses the internet because they are radicalized). Instead, focusing on how individuals can at once both exploit and engage with others to produce radicalization outcomes (both online and offline) is crucial in understanding the roles that different factors play in the radicalization process.

NIJ-sponsored research examining individual and group radicalization processes, including the role of the internet and social media within them, further underscores this point, showing variation and raising further questions as to the extent of the impact that online versus offline contacts and activities have on radicalization outcomes.[56] The University of Maryland case studies suggest a way forward in collecting time-series data on an individual's radicalization process versus cross-sectional data on an individual that tell us what actions they have taken but do not provide any sort of time order. With those time-series case studies, we can see that one individual's radical ideology was largely developed with internet activity while another was already largely radicalized before engaging with online material.[57]

Online Exploitation May Have Different Impacts on Individuals Engaging With It and Be Used Strategically To Invoke Different Responses

Findings from the Michigan State University team suggested variations in the extent to which individuals interacting or engaging with materials in virtual space may be radicalized. For example, the team's finding that individuals interacting in the same online spaces exhibited varying levels of radicalization calls into question whether engagement in and exploitation of online spaces impacts individuals within those spaces similarly.[58] Indeed, this finding brings up important considerations relating to our ability to truly isolate the role of the internet and social media in radicalization processes. Simply put, while the internet and social media provides an opportunity to engage with potentially radicalizing materials and individuals, their impact on radicalization trajectories may vary from individual to individual, as may their use in spreading radicalizing content and connections.

Spending More Time Online and on Certain Platforms May Increase Individual Risk of Engaging With Hateful Content or Serve To Mitigate Its Impact

Risk is conceptualized in this paper as factors farther upstream related to online engagement that might increase an individual's likelihood of exposure to potentially radicalizing materials. NIJ-sponsored research from the University of Massachusetts-Lowell and Arkansas State University — both of which assessed more upstream risk factors — revealed similar, yet at times divergent, findings. Both projects focused on youth online risk and seemed to suggest that spending more time online[59] and using certain websites, including YouTube,[60] may be associated with an increased likelihood of engaging with hateful or potentially radicalizing content and spaces online. Research conducted by the University of Maryland, however, suggests that the social media platforms used by individuals convicted of ideological-related crimes may vary based on ideology but otherwise seem to mirror the social media platforms used within the United States more broadly.[61] However, certain platforms, including Instagram most notably, were found to be used either less broadly by individuals exhibiting violent extremist behaviors (where verified within the University of Maryland's sample) or to be platforms in which users would frequently encounter hateful content (according to the Arkansas State research findings). This presents an important aspect to consider moving forward: On which online platforms — and within those platforms, in what forums or spaces — is the risk of exposure to or encounters with potentially radicalizing or violent extremist content or connections the greatest and why? Further, what impact does that content or those connections have on radicalization trajectories, and does that impact vary based on the amount of time spent engaging with those online networks and content?

Individual Interactions With Others Online and Individual Characteristics May Increase the Risks of Exposure to Hateful or Potentially Radicalizing Content

Related to the role of social networks in radicalization outcomes, researchers at Arkansas State University found that interaction with close friends online was associated with an

individual being more likely to see hate content online.[62] Researchers at the University of Massachusetts-Lowell, however, found that the odds of viewing racist content, specifically, were 1.7 times higher among individuals who interacted with strangers online as compared to those who did not.[63] This may be due to differences in the studies (including their methodology, study participants, and scope), but does raise important questions related to the role of social networks as both protective and potentially facilitating forces online, and individual self-selecting behaviors versus peer influence. Furthermore, this speaks to the importance of understanding individual factors that may impact radicalization trajectories, including those impacted or facilitated by online engagement. How do offline social dynamics and connections impact what individuals share online? Do interactions with strangers online imply greater disinhibition online correlated with other risky behaviors? Or are the strangers the individuals who share hateful content? In this vein, it is interesting to consider an additional finding from the Michigan State research team — namely, that a women-only Ku Klux Klan forum was a site in which building community and support around topics like heterosexual relationships, health, and religion, coupled with implicit calls for violence, may facilitate greater hatred toward constructed out-groups.[64]

Additionally, findings from both projects point to the importance of individual beliefs, characteristics, and behaviors in increasing the risk of exposure to hateful content online. The Arkansas State University team found that individuals who are white and individuals with anti-government political views showed a greater likelihood of encountering hateful content online,[65] while the University of Massachusetts-Lowell team found that youth with good academic records and "benign disinhibition" showed a greater likelihood of reporting they had encountered hateful content.[66] This, again, points to the importance of individual factors in impacting the role that the internet and social media may play in exposing individuals to potentially radicalizing content. Certain individual factors — including race, political views, and awareness of what constitutes hateful content and risky internet behaviors — may impact the extent to which individuals recognize the potential harm in the content they consume online, the behaviors that lead them to encounter it, and their reaction to and level of engagement with the hateful content they view. Potential variations from individual to individual point to the importance of developing appropriately nuanced educational and preventive strategies which address individual characteristics that may make youth more susceptible to or unaware of the potential harm in the online content they consume and the individuals with whom they engage in virtual spaces.

Gaps and Path Forward

Much remains to be explored as it relates to the role of the internet and social media in radicalization in the United States. This is especially true given the rapid rate at which social use of the internet, social media, and technology continues to evolve, as does their use by violent extremist actors. NIJ-sponsored research on the topic provides important insights and paths forward for future research to build and expand on, as detailed below.

Although findings from NIJ-sponsored research provide some insight into how violent extremist and radicalized individuals may exploit online platforms to share their ideas, grow their own networks, seek validation, and communicate with others, future research should focus on understanding when, how, and why individuals who have already radicalized use and exploit social media and virtual sites to achieve their goals or recruit and radicalize others. Such research could, for example, build on findings from the NIJ-sponsored research highlighted in this paper to examine how violent extremist individuals exploit specific social media platforms to communicate with and engage new followers or tailor their online propaganda and information dissemination strategies to target specific online communities and users.

In terms of the role that engagement with online content and social media may play in radicalization processes, future research could explore the extent to which certain types of messaging or communications have staying power among individuals who encounter or engage in them. For example, which factors may lead an individual to stay engaged in — or disengage from — online discussions and forums where violent extremist content and ideas are shared? Understanding these factors may also help further elaborate on what risk looks like in online behaviors that may expose individuals to potentially radicalizing materials and individuals virtually. This could also help bridge the gap between research that samples individuals who are engaged in violent extremist behaviors (in which we cannot say whether they were exposed to more material than an average internet user) and research that samples the general public (in which we cannot say whether greater exposure to harmful material will lead to extremist behavior in the future).

Conclusion and Policy Implications

NIJ-sponsored research examining the role of the internet and social media on radicalization underscores the importance of not viewing the internet and social media as spaces separated from individual experience and factors. Although findings from the research suggest that the internet and social media can play a unique and significant role in exposing individuals to hateful content, radical and extremist sentiments, and likeminded social networks, they also stress that individual experiences engaging and interacting with online content vary in salient ways. Although the findings detailed above are derived from studies that are not necessarily comparable, together they do illuminate central considerations for policy and practice aimed at *mitigation*, or addressing the roles that exploitation, engagement, and risk on the internet and social media may have in producing radicalization outcomes.

Consider the Role of the Internet and Social Media in Relation to Other Factors and Activities

Online behaviors, activities, and engagement do not occur in a vacuum. Understanding the role of the internet and social media in radicalization, therefore, requires understanding online exploitation, engagement, and risk as part of a larger ecosystem of interactions, individuals, and social structures. As NIJ-sponsored research has shown, even online social networks can translate into the offline space with varying impacts on violence and radicalization outcomes.[67] Rather than consider the role of the internet in isolation, policymakers and practitioners should consider the interplay between online and offline communications and engagement in developing efforts to address the influence of both on radicalization processes. As noted by the Michigan State University team, developing frameworks that integrate subcultural radicalization theories and the role of internet-based communications within them is necessary in better understanding causal mechanisms and addressing complex interactions in radicalization processes.[68]

Consider Specific Interventions Tailored to Different Types of Online Engagement

Interventions and activities designed to address the impact of the internet and social media on radicalization processes should be appropriately tailored based on the type of online engagement and the online spaces in which they are carried out. Interventions to address violent extremist exploitation of online spaces, individual engagement in online communities and content, and behaviors that put individuals at greater risk of engaging with those communities and content will necessarily differ in their activities and scope, despite remaining complementary toward one another. Although holistic strategic initiatives aimed at addressing radicalization in virtual spaces should incorporate efforts to address each of these factors, doing so requires appropriately understanding, tailoring, and potentially connecting these initiatives and their varied areas of focus.

What is more, interventions focused on the online space, much like those in the offline space, must recognize the heterogeneity that exists in ideological expressions and activities online (even within the same ideological strand, as noted by the Michigan State University team) and across different online platforms. Synthesized findings from NIJ-sponsored research focused on radicalization and the online space collectively allude to the varied impact and engagement in online spaces where violent extremist content and communities are present. They also underscore that different online platforms may be used for different purposes by different types of violent extremist ideological groupings and individuals. Crafting effective policy to address the potential impact of the internet and social media on radicalization, therefore, requires understanding how different types of actors use different types of platforms for different purposes. Further research into how different platforms are used, by whom, and for what purpose is needed to inform tailored policy responses to them. According to NIJ-sponsored research, attention to how offline dynamics may impact online engagement, and the development of proactive messaging efforts to address these circumstances, may be prudent in mitigating their impacts,[69] although their potential efficacy in doing so is unclear.

Understand When Efforts To Address Violent Extremism Online May Overlap With Broader Social Goals and Violence Reduction Efforts

Engaging with or experiencing hateful content online has different impacts on different individuals. As NIJ-sponsored research findings collectively suggest, simply engaging with or viewing hateful or violent extremist content online does not, in itself, imply a greater propensity to radicalize to violence. Although this does not negate the potential harms and issues that hateful or violent extremist content can have, it does pose important considerations for policymakers and practitioners seeking to mitigate that content's impact in virtual spaces. When dealing with online content and activity, especially given the protections afforded speech and expression in the United States, policymakers should consider whether policies and practice for preventing and countering violent extremism are the best means of addressing issues that may be hateful or concerning in nature, but that in themselves do not rise to the level of illegal or terrorist activity. This is, admittedly, a difficult task, but one that is consequential. Initiatives for countering violent extremism and terrorism can play a key role in identifying and addressing explicit terrorist exploitation and engagement and limiting the risk of individuals engaging with such content. However,

when addressing issues that are more relevant to general online safety and awareness, it may be less feasible or desirable to engage in activities for countering violent extremism or terrorism. In fact, doing so may lead to negative consequences, profiling, and stigmatization. The University of Massachusetts-Lowell team's considerations and guidelines for ethical engagement in preventing and countering violent extremism may be useful in thinking through the ethics of this type of engagement.[70]

Notes

1. For additional synthesized findings from NIJ-sponsored research on radicalization in the United States, see Allison G. Smith, "How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us," Washington, DC: U.S. Department of Justice, National Institute of Justice, June 2018, NCJ 250171, https://www.ojp.gov/pdffiles1/nij/250171.pdf; Allison G. Smith, "Risk Factors and Indicators Associated With Radicalization to Terrorism in the United States: What Research Sponsored by the National Institute of Justice Tells Us," Washington, DC: U.S. Department of Justice, National Institute of Justice, June 2018, NCJ 251789. https://www.ojp.gov/pdffiles1/nij/251789.pdf; and Kateira Aryaeinejad and Thomas L. Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization: What Research Sponsored by the National Institute of Justice Tells Us," Washington, DC: U.S. Department of Justice, National Institute of Justice (forthcoming).

2. For more, see Aisha Javed Qureshi, "Understanding Domestic Radicalization and Terrorism: A National Issue Within a Global Context," *NIJ Journal* 282, August 2020, https://nij.ojp.gov/library/publications/understanding-domestic-radicalization-and-terrorism-national-issue-within.

3. For further analysis on how research has examined radicalization online, see, for example, Charlie Winter et al., "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies," *International Journal of Conflict and Violence* 14 no. 2 (2020), https://doi.org/10.4119/ijcv-3809.

4. Research focused on the role of social networks in radicalizing individuals to terrorism or violent extremism, including previous NIJ-sponsored research, has consistently pointed out the role that online social networks and connections can play in radicalization trajectories, both in terms of groups and lone actors. For further discussion of NIJ-sponsored research addressing the role of social networks both on- and offline, see Aryaeinejad and Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization."

5. The shooter in the May 2022 Buffalo, New York, attack is a recent example of an attacker posting a manifesto online, itself drawing heavily from internet memes and message boards. See Justin Ling, "How 4chan's Toxic Culture Helped Radicalize Buffalo Shooting Suspect," *The Guardian*, May 18, 2022.

6. For discussion of different tactics discussed previously, see, for example, Peter R. Neumann, "Options and Strategies for Countering Online Radicalization in the United States," *Studies in Conflict & Terrorism* 36 no. 6 (2013): 431-459, https://doi.org/10.1080/1057610X.2013.784568.

7. Aryaeinejad and Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization."

8. Among examples of such research, see Charlie Winter, *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy* (London: Quilliam, 2015).

9. See, for example, Maura Conway, Ryan Scrivens, and Logan Macnair, "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends," *International Centre for Counter-Terrorism* (2019); Thomas J. Holt, Steve Chermak, and Joshua D. Freilich, "Assessment of Extremist Groups Use of Web Forums, Social Media, and Technology to Enculturate and Radicalize Individuals to Violence," Final report to the National Institute of Justice, award number 2014-ZA-BX-0004, January 2021, NCJ 256038, https://www.ojp.gov/pdffiles1/nij/grants/256038.pdf; and Ryan Scrivens et al., "Right-Wing Extremists' Use of the Internet: Emerging Trends in the Empirical Literature," *VoxPol*, September 21, 2022.

10. For more, see, Conway, Scrivens, and Macnair, "Right-Wing Extremists' Persistent Online Presence"; and Winter et al., "Online Extremism."

11. A wealth of research discusses different uses of the internet by violent extremists. For example, see Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38 no 1 (2015): 1-22, https://doi.org/10.1080/1057610X.2014.974948; and Winter et al., "Online Extremism."

12. Or "broadcasting of intent." See Mark Hamm and Ramon Spaaj, "Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways To Forge Prevention Strategies," Final report to the National Institute of Justice, award number 2012-ZA-BX-0001, February 2015, NCJ 248691, https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf; and Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums."

13. See discussion in the synthesized findings presented below.

14. It is important to note that the NIJ-sponsored studies discussed herein investigated different aspects associated with these four categories, focusing on different demographics, ideological strands, and characteristics.

15. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums."

16. While the researchers used the term "far-right" broadly to describe the content and ideological leanings of the web forums, they also acknowledged that the term encompasses a wide range of ideological leanings and sentiments. In addition, although

the data derived for the study came from seven far-right forums, the researchers acknowledge that, in total, eight were examined. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 4.

17. Years and posts varied based on the seven forums analyzed, with four of seven containing data derived prior to 2010 and three of seven containing data derived in 2010 and after. Only one of the seven forums contained data derived following 2015. For more information, see Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 4.

18. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 3.

19. Shuki Cohen et al., "Invisible Empire of Hate: Implicit Ideological Justifications for Violence and Hate in a Female Ku Klux Klan Online Forum," *Violence and Gender* 5 no. 4 (2018): 209-225, https://doi.org/10.1089/vio.2017.0072.

20. For example, the researchers found forums affiliated with real-world groups to demonstrate statistically significant differences in posting conspiratorial content, content targeting specific groups, and participation in real-world meetings and events (to name a select few) — with those in real-world-group-affiliated forums posting more about conspiratorial content and content targeting specific groups, and those in unaffiliated forums posting more content about participation in real-world events and meetings. For more, see Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 5-11.

21. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 35.

22. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 18-19.

23. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 36.

24. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 31-34.

25. Matthew Costello et al., "Radicalization on the Internet: Virtual Extremism in the U.S. from 2012-2017," Final report to the National Institute of Justice, award number 2014-ZA-BX-0014, January 2021, NCJ 256036, https://www.ojp.gov/pdffiles1/nij/grants/256036.pdf.

26. Matthew Costello et al., "Predictors of Viewing Online Extremism Among America's Youth," *Youth & Society* 52 no. 5 (2020): 710-727, https://doi.org/10.1177/0044118X18768115.

27. Costello et al., "Predictors of Viewing Online Extremism Among America's Youth."

28. Matthew Costello et al., "Who Views Online Extremism? Individual Attributes Leading To Exposure," *Computers in Human Behavior* 63 (2016): 311-320, https://doi.org/10.1016/j.chb.2016.05.033; and James Hawdon, Colin Bernatzky, and Matthew Costello, "Cyber-Routines, Political Attitudes, and Exposure to Violence-Advocating Online Extremism," *Social Forces* 98 no. 1 (2019): 329-354, https://doi.org/10.1093/sf/soy115.

29. Matthew Costello, James Hawdon, and Thomas Ratliff, "Confronting Online Extremism: The Effect of Self-Help, Collective Efficacy, and Guardianship on Being a Target for Hate Speech," *Social Science Computer Review* 35 no. 5 (2016): 587-605, https://doi.org/10.1177/0894439316666272.

30. Matthew Costello, Joseph Rukus, and James Hawdon, "We Don't Like Your Type Around Here: Regional and Residential Differences in Exposure to Online Hate Material Targeting Sexuality," *Deviant Behavior* 40 no. 3 (2019): 385-401, https://doi.org/10.1080/01639625.2018.1426266.

31. James Hawdon et al., "Conflict Management Styles and Cybervictimization: Extending Routine Activity Theory," Sociological Spectrum 37 no. 4 (2017): 250-266, https://doi.org/10.1080/02732173.2017.1334608.

32. Matthew Costello, James Hawdon, and Amanda Cross, "Virtually Standing Up or Standing By? Correlates of Enacting Social Control Online," *The International Journal of Criminology and Sociology* 6 (2016): 16-28, https://doi.org/10.6000/1929-4409.2017.06.03.

33. James Hawdon et al., "The Perpetuation of Online Hate: A Criminological Analysis of Factors Associated With Participating in an Online Attack," *Journal of Hate Studies* 15 no. 1 (2019): 157-181, https://doi.org/10.33972/jhs.166.

34. Matthew Costello and James Hawdon, "Who Are the Online Extremists Among Us? Sociodemographic Characteristics, Social Networking, and Online Experiences of Those Who Produce Online Hate Materials," *Violence and Gender* 5 no. 1 (2018): 55-60, https://doi.org/10.1089/vio.2017.0048.

35. For more information on the different components of the project, see Gary LaFree, "Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence," Final report to the National Institute of Justice, award number 2015-ZA-BX-0004, January 2021, NCJ 256024, https://www.ojp.gov/pdffiles1/nij/grants/256024.pdf.

36. Colleen E. Mills et al., "Social Learning and Social Control in the Off- and Online Pathways to Hate Crime and Terrorist Violence," *Studies in Conflict & Terrorism* 44 no. 9 (2021): 701-729, https://doi.org/10.1080/1057610X.2019.1585628; Thomas J. Holt et al., "Examining the Utility of Social Control and Social Learning in the Radicalization of Violent and Non-violent Extremists," *Dynamics of Asymmetric Conflict* 11 no. 3 (2018): 125-148, https://doi.org/10.1080/17467586.2018.1470661; and Aryaeinejad and Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization."

37. Mills et al., "Social Learning and Social Control in the Off- and Online Pathways to Hate Crime and Terrorist Violence."

38. Holt et al., "Examining the Utility of Social Control and Social Learning."

39. Mills et al., "Social Learning and Social Control in the Off- and Online Pathways to Hate Crime and Terrorist Violence."

40. LaFree, "Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence," 6-9.

41. Janet I. Warren et al., "The Creation of Muhajirat in America: Social Media as a Platform for Crafting Gender-Specific Interventions for the Domestic Radicalization of Women," Final report to the National Institute of Justice, award number 2016-ZA-BX-K001, September 2020, NCJ 255237, https://www.ojp.gov/pdffiles1/nij/grants/255237.pdf.

42. Janet I. Warren et al., "Operationalizing Theory: A Moral-Situational Action Model for Extremist Violence," *Journal of Threat Assessment and Management* 5 no. 4 (2018): 205-226, https://psycnet.apa.org/doi/10.1037/tam0000118.

43. Warren et al., "The Creation of Muhajirat in America," 19-20.

44. Warren et al., "The Creation of Muhajirat in America."

45. See NIJ award number 2016-ZA-BX-K001 and the discussion in Kateira Aryaeinejad and Thomas L. Scherer, "Evaluating and Assessing Terrorism Prevention Programs: What Research Sponsored by the National Institute of Justice Tells Us," Washington, DC: U.S. Department of Justice, National Institute of Justice (forthcoming).

46. Conversation with the project lead, July 2022.

47. Conversation with the project lead, July 2022.

48. Neil D. Shortland, Nicholas Evans, and John Colautti, "A Public Health Ethics Model of Countering Violent Extremism," *Terrorism and Political Violence* 33 no. 2 (2021): 324-337, https://doi.org/10.1080/09546553.2021.1880231.

49. Nigel Harriman et al., "Youth Exposure to Hate in the Online Space: An Exploratory Analysis," *International Journal of Environmental Research and Public Health* 17 no. 22 (2020), https://doi.org/10.3390/ijerph17228531; and Costello et al., "Radicalization on the Internet."

50. Specifically, the fact that those in low- and medium-risk communities were found to be more likely to engage with and disseminate content online, whereas those in the high-risk communities (i.e., those undertaking violent action) were less likely to be involved in online spaces. This may suggest, as the researchers note, that individuals active in online spaces are less likely to undertake acts of violence against other people. See Warren et al., "The Creation of Muhajirat in America," 32.

51. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 18-19.

52. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 5-10.

53. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums."

54. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 35.

55. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums," 19.

56. For detailed discussion, see Aryaeinejad and Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization."

57. Although these findings varied based on motivation and time periods. See LaFree, "Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence," and Mills et al., "Social Learning and Social Control."

58. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums."

59. The Arkansas State University team's research was based on hours alone, while the University of Massachusetts-Lowell team found that youth who spent three or more hours per day online had 2.4 times the odds of reporting exposure to hate content on a website or social media platform as compared to those who spent less than three hours online per day. See Costello et al., "Predictors of Viewing Online Extremism Among America's Youth"; and Harriman et al., "Youth Exposure to Hate in the Online Space," 9.

60. In addition to YouTube, the University of Arkansas team also found that Reddit and Snapchat proved consequential. The YouTube algorithm's suggestions of additional video content based on videos recently viewed and relative anonymity are suggested as reasons for which the platform may lead to greater exposure to hate content. Costello et al., "Predictors of Viewing Online Extremism Among America's Youth," 720.

61. LaFree, "Social Learning and Social Control in the Off and Online Pathways to Hate and Extremist Violence," 6-9.

62. Costello et al., "Predictors of Viewing Online Extremism Among America's Youth."

63. Harriman et al., "Youth Exposure to Hate in the Online Space," 9.

64. Cohen et al., "Invisible Empire of Hate."

65. Costello et al., "Predictors of Viewing Online Extremism Among America's Youth."

66. This, of course, could be due to heightened awareness among individuals displaying these factors that the content they were engaging with was, in fact, hateful in nature. Personal conversation with project lead, July 2022.

67. For an overview, see Aryaeinejad and Scherer, "The Role of Social Networks in Facilitating and Preventing Domestic Radicalization."

68. Thomas J. Holt, Joshua D. Freilich, and Steven M. Chermak, "Internet-Based Radicalization as Enculturation to Violent Deviant Subcultures," *Deviant Behavior* 38 no. 8 (2017): 855-869, https://doi.org/10.1080/01639625.2016.1197704.

69. Holt, Chermak, and Freilich, "Assessment of Extremist Groups Use of Web Forums."

70. Shortland, Evans, and Colautti, "A Public Health Ethics Model of Countering Violent Extremism."

About the Authors

Kateira Aryaeinejad specializes in research on violent extremism, focusing on research processes, global and local dynamics, and connecting rigorous research to policy and practice. Her work has focused on topics ranging from the evolution of and local support for violent extremist groups and narratives, online and offline communications, and peacebuilding and conflict dynamics. She holds an M.A. in International Peace and Conflict Resolution with a concentration in International Conflict Management from American University's School of International Service.

Thomas Leo Scherer is the research director for fp21. His work is focused on identifying and conducting high-quality research to improve U.S. foreign policy. He has previously worked on violent conflict research at the Center for Peace and Security Studies at the University of California San Diego and at the United States Institute of Peace. He has a Ph.D. in International Relations from Princeton University.