The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization

Testimony to the U.S. House of Representatives Subcommittee on Counterterrorism and Intelligence

Kurt Braddock
School of Communication
Center for Security, Innovation, and New Technology
Center for Media and Social Impact
American University

To Chairman Pfluger, Ranking Member Magaziner, and the distinguished Members of the subcommittee, I would first like to thank you for the invitation to appear before you. Issues related to recruitment and radicalization via the internet have pervaded the study of violent extremism for decades. It is heartening to know that legislators remain cognizant of these complex processes and determined to undermine them, when and where possible.

I would also like to note that any claims or statements I make in my written or spoken testimonies do not necessarily reflect the position of American University, the School of Communication, or any research center with which I am affiliated. The testimony I provide here is based on 20 years of my findings as a researcher of radicalization and terrorism.

I have studied domestic left-wing and right-wing extremist groups, foreign terrorist entities of nearly every political or religious ideology, lone-actor terrorists, and everything in between. Incidentally, it is the time that I have spent studying diverse kinds of terrorist actors that has helped me to understand radicalization processes in a systematic manner. The first, and most difficult fact to confront is that the social and psychological processes by which individuals come to support the use of terrorism are as varied as the individuals that experience them. As such, no single hearing would be sufficient to comprehensively describe these issues.

Nevertheless, after 20 years of observation, interviews, controlled experiments, and data analysis, I have noticed some patterns among not only cases of radicalization and terrorism, but also the contexts in which they have occurred. It is these commonalities on which I will focus my testimony. Rather than attempt to offer every detail related to why radicalization occurs (which can be discussed in some detail during the hearing itself, should members wish to discuss it), I will be focusing my testimony along three key themes that I feel would be of interest to the committee:

(1) Psychological radicalization to violence and its facilitation online,
(2) Social media as a communicative mechanism for fostering radicalization, and
(3) Responding to the threat of online recruitment and radicalization by malicious actors.

1. Radicalization to Violence: Psychological Processes

Before delving into the *radicalization* process as it plays out in online spaces, conceptual disagreements about the nature of radicalization – among both researchers and security practitioners – require that we utilize a working definition. For the purposes of this testimony, I define radicalization as a social and psychological process by which an individual comes to adopt beliefs and attitudes that are consistent with an extremist ideology. It is important to note that radicalization, per se, does not automatically result in violent behavior on the part of the radicalized. In fact, the vast number of individuals who undergo radicalization never support or engage in violent activity. Radicalization of beliefs and attitudes may render a person a greater risk for engaging in terrorism, but this is by no means a forgone conclusion.[1]

An extended form of radicalization – called *radicalization to violence*[2] – depicts this process. Radicalization to violence involves not only a change in beliefs and attitudes such that they are consistent with those of violent extremists, but also the added intention (and possible opportunity) to carry out a violent attack against civilian targets. To reiterate: not all who undergo radicalization turn to violence, but it does serve as a risk factor.

Given this distinction, and under the assumption that the primary concern of this subcommittee is to prevent violence against American citizens rather than deplorable (yet perfectly legal) beliefs and attitudes, my testimony concerns *radicalization to violence* – that is, radicalization of behavior – rather than radicalization of beliefs and attitudes.[3]

Given this, please allow me to turn to psychological mechanisms by which radicalization can occur. As noted above, radicalization processes are various, and are a product of several individual-, group-, and societal-level factors. Still, decades of research on political violence reveals several social and psychological processes that may be affected by the messages with which an individual engages. These processes include (but are not limited to) *self-deindividuation*, *other-deindividuation*, *dehumanization*, and *demonization*. Although these processes are not unique to the online domain, the polarizing nature of social media (see below) can facilitate and catalyze these processes at scale.

First, self-deindividuation[4] is a psychological process by which a person comes to believe that the importance of their identity as a member of some group has superseded their identity as an individual. That is, they see themselves as part of something bigger or more important than themselves, and are therefore willing to make individual sacrifices to their own well-being

---

[1] Ghayda Hassan, Sebastien Brouilette-Alarie, Seraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnpaul Varela, et al. "Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence," *International Journal of Developmental Science* 12 (2018): 71-88.

[2] John Horgan, *The Psychology of Terrorism*, 2nd ed. (Oxon, UK: Routledge, 2014).

[3] See, for example, Clark McCauley and Sophia Moskalenko, "Understanding Political Radicalization: The Two-Pyramid Model," *American Psychologist* 72(3) (2017), pp. 205-216.

[4] Originally in Max Taylor, *The Terrorist* (Lincoln, NE: Potomac Books, 1988); for a summary of these processes, see Chapter 5 in Elyamine Settoul and Thierry Balzacq. *Radicalization in Theory and Practice: Understanding Religious Violence in Western Europe*. (Ann Arbor, MI: University of Michigan Press, 2022).

(including personal safety) to support the group of which they are a part. In the context of radicalization to violence, individuals who self-deindividuate while engaging with extremists online may come to believe themselves to be part of an important social movement, their membership in which is the central part of their identity. This may render them more ready to engage in violence on behalf of that movement.

Other-deindividuation relates to a process by which an individual comes to perceive members of some outgroup (e.g., those depicted as enemies) as lacking individual traits. Instead of perceiving those people as individual human beings, they are instead perceived as a homogenous mass of "them." By characterizing an outgroup in this way, extremists can psychologically prepare their recruitment or radicalization targets to harm them, should the need arise.

Related to this, dehumanization[5] is the psychological process by which an individual comes to perceive members of the outgroup to be non-human, thereby suggesting they are not worthy of the respect bestowed upon fellow humans. Often, this is prompted by speakers' characterization of the outgroup as being animals, vermin, or some other organism worthy of derision and hate. When an outgroup is discussed in these terms over time, audiences come to lose their perceptions of the outgroup's humanity, which likewise facilitates their willingness to harm them, should the group require it.

Finally, demonization[6] relates to a psychological process whereby an individual comes to perceive others as embodying evil. When an outgroup is characterized as evil, particularly if an individual believes that their ingroup is charged with defending some constituency, it becomes easier for that individual to commit violence against that group.

Self-deindividuation, other-deindividuation, dehumanization, and demonization are not the only psychological processes that can occur when an individual undergoes radicalization to violence, but many cases of terrorist violence indicate that they are relatively common among the violent.

Given that the purpose of this hearing is to understand recruitment and radicalization in the online space, however, it is useful to consider the features of the internet generally, and social media specifically, that facilitate these processes.

2. Social Media as a Mechanism for Fostering Radicalization to Violence

Understanding the psychology of radicalization to violence requires the understanding that a consideration of "online" versus "offline" radicalization is a false dichotomy.[7] By distinguishing processes that occur in an online environment from those that occur away from a computer screen incorrectly suggests that these phenomena are distinct. In truth, individual trajectories

---

[5] See Nour S. Kteily and Alexander P. Landry, "Dehumanization: Trends, Insights, and Challenges," *Trends in Cognitive Sciences* 26, no. 3 (2022): 222-240.

[6] See Roger Giner-Sorolla, Bernhard Leidner, and Emanuele Castano, "Dehumanization, Demonization, and Morality Shifting," in Michael A. Hogg and Danielle L. Blaylock, eds., *Extremism and the Psychology of Uncertainty* (Hoboken, NJ: Wiley, 2011), Chapter 10.

[7] Joe Whittaker, "Rethinking Online Radicalization," Perspectives on Terrorism 16, no. 4 (2022), 27-40.

towards terrorism are often driven by activities that take place over time in both the real-world and online domains.

Still, there are some phenomena that are unique to the online sphere generally (and social media specifically) that lend themselves to our understanding of how online engagement with malicious actors and problematic content contributes to the radicalization process. In this section, I outline some of these processes and phenomena, with a specific focus on social media, how its revenue streams are structured, and how online engagement and the commodification of attention combine to form the perfect storm for radicalization to violence when malicious actors engage with vulnerable audiences.

The primary means by which large social media platforms generate revenue is through advertising.[8] To generate income, these large companies (e.g., Meta, Twitter/X) allow advertisers to appear among the posts to which users are engaged, and when those advertisements appeal to a user, they may pay closer attention to that ad (measured in clicks or amount of time viewing the ad) or purchase the product or service being offered. To maximize the value of an advertisement, the social media platforms develop models of their users based on previous online engagement, thereby allowing them to promote advertisements that will be most appealing. In this way, advertising space on social media platforms is valuable to the degree that the platform can attract views and engagement from its users.

Because attention has been effectively commodified, the social media platforms are financially incentivized to prioritize and feature content that is likely to arouse thoughts and emotions that promote engagement. In many cases, this content takes the form of messaging with which the user has previously engaged, news that will evoke engaging feelings like anger[9] or otherwise subconsciously persuade the user to keep interacting with the platform.[10] Moreover, the algorithms that determine the basis upon which users are recommended additional content are designed to keep them in ideological echo chambers in which the messages to which they are exposed grow increasingly extreme and no dissenting voices can ever be heard.[11]

When this content is political or ideological – contexts in which disinformation is abound – users can develop increasingly extreme beliefs and attitudes about the use of violence against perceived enemies on the basis of false perceptions and imagined grievances. In this way, the cultivation of echo chambers in the online space due to the revenue structures of social media platforms builds to a "perfect storm" of engagement, isolation, and anger that can lead to the

---

[8] Amanda Raffoul, Zachary J. Ward, Monique Santoso, Jill R. Kavanaugh, and Bryn Austin, "Social Media Platforms Generate Billions in Dollars in Revenue from U.S. Youth: Findings from a Simulated Revenue Model," *PLOS One* 18, no. 12 (2023), e0295337.

[9] For example, see Jacquelien van Stekelenburg, "Radicalization and Violent Emotions," *American Political Science Association Politics Symposium* (2017).

[10] For a discussion related to subconscious advertising, see Anne-Sophie Bayle-Tourtoulou and Michel Badoc, *The Neuro-Consumer: Adapting Marketing and Communication Strategies for the Subconscious, Instinctive, and Irrational Consumer's Brain* (London: Routledge, 2020).

[11] Michael Wolfowicz, David Weisburd, and Badi Hasisi, "Examining the Interactive Effects of the Filter Bubble and the Echo Chamber on Radicalization," *Journal of Experimental Criminology* 19 (2023): 119-141.

aforementioned psychological processes (i.e., deindividuation, dehumanization, demonization), thereby increasing risk for radicalization to violence.

3. Responding to the Threat of Online Recruitment and Radicalization to Violence

Although the online space serves to facilitate several processes associated with radicalization to violence, there is an abundance of research on steps that can be taken to mitigate the likelihood that the online space (particularly social media) can be leveraged by extremists to recruit and radicalize target audiences.

First, several studies have demonstrated that the responsible moderation of some content, primarily in the form of content takedowns and user bands, can reduce the impact of malicious content.[12] These studies have collectively demonstrated that when social media platforms work with experts in extremist messaging, media, and psychology to identify content that poses a risk for audience radicalization, the content is not distributed as widely and the malicious actors are less likely to reach their target audiences. That said, the prevalence of malicious content online suggests that exclusive reliance on content moderation would not be sufficient for reducing the efficacy of recruitment and radicalization efforts. Instead, moderation should be considered only a tool in the overall toolkit of platform administrators.

Rather than rely solely on a reactive approach like content moderation, there is also research to suggest that prophylactic strategies that seek to increase audience resistance to extremist content would be particularly effective. Specifically, media literacy initiatives[13] designed to teach audiences – particularly young audiences – about how malicious actors may develop content designed to lead them to violence could be particularly useful. Given the increasingly young age at which many children are becoming digitally literate, it would behoove interested parties to consider media literacy campaigns as early as is reasonable.

Finally, there exists a specific counter-persuasion strategy in which users are exposed to weakened versions of the extremist messages to which they will later be exposed when they are online.[14] Several decades of research have shown that when audiences are told about the content they will encounter (or the strategies that malicious actors may use to distribute that content), and are provided with counter-arguments against it, they are substantially less likely to be

---

[12] For a current review of these practices, see latest articles in Studies in Conflict and Terrorism, especially Maura Conway and Stuart Macdonald, "Introduction to the Special Issue: The Practicalities and Complexities of (Regulating) Online Terrorist Content Moderation," *Studies in Conflict & Terrorism* (2025, online). See also Heather Wolbers, Christopher Dowling, Timothy Cubitt, and Chante Kuhn, "Understanding and Preventing Internet-Facilitated Radicalisation," *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, no. 673.

[13] For an early synopsis, see Jan-Jaap van Eerten, Bertjan Doosje, Elly Konjin, Beatrice de Graaf, and Marielle de Goede, *Developing a Social Media Response to Radicalization: The Role of Counter-Narratives in Prevention of Radicalization and De-Radicalization* (Amsterdam, NL: Colophon), 108.

[14] Josh Compton and Kurt Braddock, "Inoculation Theory and Conspiracy, Radicalization, and Violent Extremism," in Sergei A. Samoilenko and Solon Simmons, eds., *The Handbook of Social and Political Conflict* (Hoboken, NJ: John Wiley and Sons, 2025).

persuaded by it.[15] This approach would be particularly fruitful for dealing with propaganda and disinformation produce with generative artificial intelligence,[16] which can be particularly difficult to identify and resist without proper training.

The written testimony I have provided above represents only a small drop in the bucket of our collective knowledge related to the online sphere, radicalization to violence, and the increasingly complex ways that extremist groups are targeting vulnerable audiences. However, as extremists develop increasingly sophisticated methods for recruiting and radicalizing audiences to violence, so too must we develop increasingly sophisticated methods for undermining them.

Note that additional scholastic references for the concepts described above are available upon request. I would also be happy to provide the committee with additional information concerning radicalization to violence more generally and the role of the internet in facilitating it.

[15] For experimental evidence in the realm of violent extremism, see Kurt Braddock, "Vaccinating against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda," *Terrorism and Political Violence* 34, no. 2 (2022): 240-262.
[16] Stephane J. Beale and Lewys Brace, "AI Extremism: Technologies, Tactics, Actors," VOX-Pol Report (2024). https://dial.uclouvain.be/pr/boreal/object/boreal:291289.