March 31, 2022

Dr. Brian Hughes
Associate Director
PERIL
American University
Washington, DC

Statement for the Record by Brian Hughes, Associate Director of the Polarization and Extremism Research and Innovation Lab (PERIL) at American University

Introduction

The Polarization and Extremism Research and Innovation Lab (PERIL) at American University in Washington, DC, thanks the Select Committee to Investigate the January 6th Attack on the United State Capitol for the opportunity to contribute to this critical investigation. We are grateful for your work on what we believe to be an existential attack on American democracy.

PERIL is an applied research lab, which studies topics ranging from political violence to social polarization, conspiracy theories, and socially maladaptive fringe subcultures. We use this research to craft and test interventions aimed at reducing social risks associated with extremism. Dr. Brian Hughes (the author of this testimony) serves as Associate Director for the lab, co-founded with Dr. Cynthia Miller-Idriss in 2019. Dr. Hughes heads research and interventions which focus on the use of digital communication technology in the formation and operational execution of extremist activity and political violence.

We should recognize that the events of January 6th were facilitated by larger trends in the communication technologies with which Americans organize their social lives and, increasingly, their political activity. The unique features of these technologies must be taken into account in all work—legislative, law enforcement, and intelligence—to reduce the risk of similar future events.

Overview

Observers of the January 6th assault on the Capitol witnessed troubling signs of fraternizing and even cooperation between a variety of extremist groups and unaffiliated protestors. This strange coalition of unlawful militias, white supremacists, QAnon conspiracy theorists, Proud Boys and ordinary voters highlight the strange and unanticipated ways in which domestic violent extremism scenes in the United States are fragmenting and reassembling. The transformation is taking place both organizationally and post-organizationally, through distributed, ad-hoc networks online.

On the organizational side, political violence is emerging from a loose new coalition that spans the extremist spectrum in ways that muddle the ideological basis typically understood to be at the root of terrorist and extremist violence. On the post-organizational side, exposure to extremist content and radicalization into ideologies and violence outside the boundaries of organized groups is increasing—largely through online encounters with propaganda, disinformation and extremist ideas.

In many ways, the phenomenon is nothing new. Extremist scenes and movements have experienced internal fissures, infighting and fragmentation for years due to differences in beliefs about tactics (such as the use of violence), conflicting views on particular parts of their ideology (such as about Jews and whiteness) or restrictions on who can be members (such as women). Increasingly, this conflict is occurring not just across relatively bounded groups but also among a broad muddling of ideological beliefs within domestic and international extremist scenes, movements and individuals. These trends are different from previous iterations of extremist fracture and reformation.

There are many reasons for the increased muddling of ideological rationales: the increasing ability of cross-ideological concepts to mobilize violence, rising event-driven violence, and tactical convergence, to name a few. This testimony will focus on the role of communication infrastructure in fostering these new forms of cross-ideological extremist cooperation.

The Role of Digital Communication in Cross-Ideological Mobilization

The Internet offers essential technological features—sometimes called affordances—that enable and even promote the integration of disparate political and cultural groups. There are three such key affordances contributing to the emerging integration of extremism scenes and mainstream Americans: the hyperlinked structure of the Web, network dynamics governing digital platform growth, and the role of algorithmic automation in serving content to internet users.

Hyperlinks Connect Disparate Beliefs and Groups

A hyperlink, or more colloquially a “link,” is a short line of code, which allows an internet user to jump between webpages with the click of a mouse. Hyperlinking has been essential to the

operation of the World Wide Web since its inception at the CERN lab in 1989. Hyperlinks allow any two data points to be connected with trivial ease. This allows Web users to become, in the words of internet visionary Vannevar Bush, "trail blazers" through pathways of information, creating chains of logic and association, which others may follow and learn from. However, these pathways are only as logical or accurate as their creators. It is just as easy to blaze a trail of illogic and disinformation. We now live in an age of *argumentum ad hyperlink*. Readers rarely click hyperlinks to investigate even the most basic assertions of a headline. In one study, hyperlinks within news stories linked to explicitly mentioned sources less than 50% of the time, and less than one third of all sources were hyperlinked at all. Readers seem to take the mere presence of a hyperlink as adequate support for key claims.

By the same token this structure of hyperlinking is capable of putting disparate political factions side-by-side. Click a link in your natural health Facebook group and you may hop to a QAnon thread. Click a link on the QAnon thread about "The Storm" (QAnon's imagined day of reckoning) and you may just as easily find an imageboard dedicated to violent insurrection. In the mind of a vulnerable user, these hyperlinked connections imply legitimate affinity between the groups. Conspiracy theories thrive under these conditions, as vague associations and innuendo weave paranoid stories based on a digitally falsified sense of cause-and-effect. The movements which intermingled so freely on January 6th demonstrate precisely this ideological eclecticism and epistemic nihilism.

The affordances of the hyperlink make it orders of magnitude easier for someone with a grievance to leapfrog from left-wing military anti-interventionism to New World Order reptilian conspiracy theories to anti-civilizational deep ecology to far-right "national anarchism" to the boogaloo movement and beyond. And the online nature of these ideological explorations makes it less likely that contradictions will ever be reconciled. Instead, they accrue in an ever-evolving set of fragmented ideological commitments, extremist, identities and conspiracy beliefs.

Power Laws, Network Effects, and Digital Mobs

Digital networks do not grow in the same way that offline networks do. Thanks to something called the "power law dynamic," a handful of nodes in any digital network tend to receive the lion's share of traffic and attention. Power law dynamics are not universal to online platforms, but this winner-takes-all arrangement tends to be no less true for extremist channels than for mainstream blogs or online bookstores. Extremists flocked to Twitter, Facebook, YouTube and other platform monopolies for the same reason that brands and would-be influencers did: no other online audience came close in terms of size.

The power law dynamic is aided by another dynamic known as "network effect." As an online network grows, its value to users can increase exponentially. This attracts even more users at an ever-increasing rate, until the platform comes to dominate its niche in the digital ecosystem. This is one reason why, for example, the far right swarmed specifically to Telegram following a

post-Jan. 6th rash of deplatforming on Twitter and Facebook. Telegram already offers a rich network of radical and extremist users, making it a valuable communication resource. As more users flock there, Telegram's value as a communication tool increases, which further incentivizes potential users to create accounts. This serves to produce online destinations for both unaffiliated individuals, ordinary voters, and dedicated extremist recruiters and propagandists. The network effect, in other words, brings together disparate and muddled political tendencies in densely connected online communication spaces.

Algorithmic Automation and the Power of Suggestion

Automation is the affordance that enables digital media to be altered, disseminated, and even created through the use of templates and algorithms. It makes possible everything from WordPress sites to Instagram filters, Netflix recommendations and the bot accounts that plague social media. Automation is what enables the Internet to operate at its current scale. It would be simply impossible to manually design—much less program—our present volume of digital content.

But by now the dangers of algorithmic recommendations are well known. Platforms like Facebook are notorious for introducing users to radical and extremist pages. YouTube's role in providing content "rabbit holes" to extremism is also documented. Even when automated recommendations do not favor outrage, fear, and loathing, their tendency is to aggregate and segregate people of similar persuasions. This encourages radicalization through processes of outbidding, "risky shifting," and other dynamics related to what Sunstein calls the "Law of Group Polarization." Hence, extremist tendencies become integrated with one another and isolated from mainstream discourse.

Automation also facilitates the growth of political extremism via the professional gloss it grants extremist media. Automated web design and photo editing enable the fringes to mirror the mainstream. In the pre-digital age, extremist content often came packaged in amateurish design: the photocopied 'zines of 1980s skinhead culture or the recognizably self-published appearance of militia manuals. Today, these visual cues are increasingly rare, as our neighborhood boutiques use the same web design templates as white supremacist blogs and militia outfitters. This dynamic only helps to further normalize extremism within the fabric of our society. In turn, this makes alliances between "ordinary" voters and extremist groups more likely when mobilizing issues and events arise.

Recommendations

Social media and other digital communication technologies are still relatively new phenomena. Their impacts are still being understood, and therefore responding to their antisocial potentials

warrants innovative—and even bold—measures. Public mood and political will may render some of these recommendations more realistic than others.

A Public Health Approach to Reduce Vulnerability

Policymakers are unlikely to solve tomorrow's problems of extremism with surveillance and securitized tools developed in yesterday's battles. On the contrary, the primary hope for reducing pressing extremist threats to democracy is through early prevention and intervention such as attitudinal inoculation. This includes reducing people's vulnerability to online manipulation, providing digital and media literacy training for all, and reducing the kinds of moral disengagement and dehumanization that are demonstrated precursors to political violence.

Resilience resources should focus on fundamental community health as well as violence prevention. In much the same way that our schools and media have been encouraged to tackle topics such as drugs, sexual abuse, and bullying, youth must be taught how to recognize and resist the misinformation and disinformation that run rampant on social media. This training must be evidence-based, and routinely updated and tested to reflect the rapidly shifting field of extremist politics in the United States. It should focus on the holistic well-being of our communities, rather than mere last-minute interventions when violence is on the cusp of occurring.

Increased Government Oversight of Digital Platforms

Social media platforms often operate as "black box" technologies. Social media companies routinely make choices which actively foster and encourage connection between some individuals and groups, while discouraging access to other groups or bodies of information. We know that these technologies connect people with one another and with political propaganda as was never before possible. But we do not know exactly how they do so. The design and engineering of these platforms affect consequences remain hidden from proper oversight. Their effects on the public can only be ascertained partially, long after their effects have already been felt. Frances Haugen's whistleblowing testimony to congress in late 2021 presents many such examples. January 6th is yet another example of black box communication technology wreaking profound damage to our society's well-being.

Given the profound influence these platforms have on Americans' social and political life, their engineering and design choices warrant much stricter oversight. In the same manner that drug-makers coordinate with the Food and Drug Administration prior to their drugs reaching the market, social media companies might be obliged to coordinate their design and engineering strategies with the Federal Communication Commission to reduce the risk of adverse effects such as those discussed in this testimony. This is not to suggest that government be given the

opportunity to read Americans' private online communication. Rather, it is a call for oversight into the basic engineering of the algorithms that feed Americans into social and political networks, the likes of which were seen on the January 6th assault on the Capitol.

Reform of Section 230

Under Section 230 of the Communications Decency Act, interactive computer services enjoy indemnity against the use of their platforms for many criminal purposes. Recently, the Fight Online Sex Trafficking Act (FOSTA) and Stop Enabling Sext Traffickers Act (SESTA) carved out exceptions to Section 230, to ensure that online platforms cannot profit from human trafficking, prostitution, and related crimes. Similar carve-outs to Section 230 should be pursued in response to acts of political violence.

As described above, the threat to our democracy posed by political violence organized and inspired through digital communications platforms is exacerbated by the very engineering and design choices of these platforms. Social media companies like Meta (Facebook) have repeatedly been shown to adjust their algorithms to provoke feelings of outrage and anger from unwitting users. These companies have likewise repeatedly been shown to adjust their algorithms in ways that favor political extremism, conspiracy theory culture, and other publicly detrimental social attitudes. As demonstrated on January 6th, the consequences of these design and engineering choices can have negative impacts on the foundations of American society, which are even more profound than those posed by human trafficking and related crimes. Tech companies must not be allowed to profit from violent threats to American democracy. Section 230 must be reformed to discourage such activities.

Conclusion

It may be even more challenging to alter the fundamental causes of treasonous behaviors like those seen on January 6th, 2021 than it is to hold its organizers criminally accountable. However, doing so is critically necessary for the future of American democracy. Congress wields unique power to hold tech companies acceptable for the externalities of their highly profitable business. I urge this committee to recommend that legislative and regulatory steps be taken to ensure that bad actors such as those responsible for January 6th do not have the tools of mass digital communication to enact future assaults on the foundations of American values and democracy.