Academic and Practical Research Working Group
White Paper: Extremism Research Horizons

Author: The International Centre for the Study of Radicalisation, King’s College London
January to June 2021
Six days into 2021, the United States (U.S.) was rocked by an unprecedented assault by right-wing extremists that struck at the heart of its constitutional system. The mob that stormed the U.S. Capitol Building on January 6, seeking to overturn the results of the November 2020 presidential election, comprised a heterogeneous group of violent far-right extremists, militia members, white supremacists, QAnon conspiracy theorists, as well as more run-of-the-mill supporters of outgoing President Donald Trump. While unsuccessful in its ultimate aims of reversing the election results, the incident represented a culmination of several trends within the Western (and particularly American) far-right ecosystem that scholars and practitioners of counterterrorism and preventing/countering violent extremism (P/CVE) have been warning of for years.

These events were also a wake-up call to tech companies about the ways in which extremists had been exploiting their platforms with a view to sharing mis- and disinformation and facilitating processes of radicalization and violence. Hence, what followed January 6 was an unprecedented response from the tech sector, with a massive effort to remove extremist content and “deplatform” certain far-right extremist voices. Most notably, President Trump himself was suspended from Twitter and Facebook.

The impact of this deplatforming intervention has yet to be fully measured and assessed, but in many ways, it appears to have been fairly ephemeral. Recent research indicates that like jihadist extremists before them, far-right activists have attempted to innovate and adapt to meet any new constraints in their information environment, with many seeming keen to learn from the failures of January 6 to improve their chances of survival online as well as engage in more effective activism in that space. At the same time, the measures employed against them by tech companies in the wake of January 6 have reignited debates about the tradeoffs between security and civil liberties such as free speech, raising fears among critics that “Big Tech” lacks the requisite legislative oversight to fairly and effectively moderate content.

Introduction
Debates such as these will likely grow more pronounced in the future as terrorists and violent extremists from across the ideological spectrum further capitalize on new technologies ranging from cryptocurrency to 3D printing. Counterterrorism efforts, meanwhile, will likely come to rely more heavily on big data and artificial intelligence (AI)-driven technologies, raising various ethical challenges. To prepare for the future of terrorism, one need only to look to the past and see that technological innovations have always been instrumental to acts of terror—and efforts to prevent them.

This white paper maps these continually shifting dynamics, drawing on proceedings from meetings of the Academic and Practical Research Working Group of the Global Internet Forum to Counter Terrorism (GIFCT), the work of the Global Network on Extremism and Technology (GNET), and original desk research. In doing so, it identifies key emerging trends and research priorities related to violent extremism, counterterrorism, and the role of the internet in these spaces. The paper is divided into three sections that respectively examine innovations in violent extremism, new developments in extremist outreach and messaging, and new research and priorities as they relate to preventing terrorist use of the internet (PTUI).
Section 1

Innovations in Online Violent Extremism

The storming of legislative buildings is hardly unique in world history and thus the January 6 assault on the U.S. Capitol is not a form of terrorist innovation per se. However, the January 6 assault exemplified several notable trends in far-right extremism that had not before manifested so prominently within the United States. It demonstrated that the American (and, to a large extent, global) far-right is a movement radicalized and mobilized largely through social media, that is relatively heterogenous, and that actively seeks support from veterans and active-duty military service members.

One cannot understand January 6 without examining the role of the internet. Scholars have long warned that social media algorithms and lax content moderation have fueled far-right radicalization in the West.\(^1\) The January 6 rallies in particular were planned online well in advance following a tweet from President Trump encouraging protests on that day.\(^2\) Most notably, many of those present in the Capitol mob remained online during the assault itself, meaning that more than 85 percent of the criminal complaints filed in relation to the Capitol assault included some form of evidence from social media.\(^3\) Researchers Jonathan Lewis and Bennett Clifford note that the high-degree of self-incriminating evidence posted by insurrection participants speaks to their poor operational security and naivete about the seriousness with which federal law enforcement would respond, “and more concerning, extremists’ deeply-held belief that their actions were legitimate.”\(^4\) They also note that the subsequent indictments, which draw heavily from social media, will teach far-right extremists how to improve online operational security (OPSEC) moving forward, a finding supported by Daniel Milton and Audrey Alexander, who identified a new emphasis on OPSEC in far-right Telegram channels after January 6.\(^5\)

The January 6 assault was also emblematic of the relative demographic and socioeconomic diversity of the far-right movement, and particularly of the important roles that women play in it. The mob that stormed the Capitol was overwhelmingly white and male, with a good number of participants that were well-educated and socioeconomically privileged. Additionally, while only 13 percent of federal cases related to the January 6 incident have been brought against women,\(^6\) certain women were particularly prominent in the day’s events. United States (U.S.) Air Force veteran Ashli Babbitt,
shot and killed by a Capitol police officer, has since become a martyr for elements of the far-right who, Marc-André Argentino and Adnan Raja note, have in many instances borrowed from the imagery and rhetoric of Black Lives Matter (BLM) to lionize the slain white woman in what is a growing trend of far-right appropriation of BLM aesthetics. Devorah Margolin and Chelsea Daymon likewise note that women helped organize the January 6 protests and also took part as both individual participants and members of militias, upending gender stereotypes in the process.

While far-right ideologies are often misogynistic and relegate women to childrearing and homemaking roles, recent research has shown that women have emerged as some of the most prominent proponents of far-right ideologies, particularly in the context of the QAnon movement. Argentino and Blyth Crawford note that women helped bring the conspiracy theory from obscure message boards onto social media and YouTube channels popular with Trump supporters. They also played a crucial role in softening QAnon’s image to appeal to generally non-extremist demographics, including Instagram influencers and traditional healing communities. Of the 97 candidates running for office nationwide in 2020 who supported or gave credence to QAnon, 37 were female, and the only two QAnon-sympathetic individuals to win seats in Congress were women. Argentino and Crawford predict that in the near future, the presence of these women in Congress will embolden more QAnon-supporting females to run for office.

Another demographic that was notably represented among the Capitol insurrectionists was that of veterans, who constitute roughly 10 percent of the defendants charged to date (though this is slightly less than their proportion of the overall U.S. population). Of this number, nearly 40 percent were affiliated with violent organizations or militias like the Proud Boys and Oath Keepers, which actively recruit veterans for their martial and organizational skills and count veterans among their leadership. This, in addition to the participation of a National Guardsman and reservist in the January 6 insurrection, has contributed to concerns within the Pentagon of extremism within military ranks, prompting Secretary of Defense Lloyd Austin to launch an internal review.

Research shows that the problem of extremist service members is not limited to the U.S. Rather, it is equally if not more relevant in many European countries. A series of high-profile cases of extremism in the German security sector has led to the disbandment of an entire company within the German
army’s elite commando force and, more recently, the disbandment of a Frankfurt police unit. As journalist Florian Flade noted in June, “The potential threat posed by weapons and ammunition stolen from military or police stockpiles has not received enough attention from the security service until recently.” Separately, in Belgium, a soldier with far-right views went on the run after stockpiling weapons from his base in April, sparking a month-long manhunt (when his body was eventually discovered, hundreds of far-right supporters marched in his name and erected shrines). Likewise, in France, over 1,000 former service members, including 20 retired generals, penned an open letter in April warning of a coming civil war, earning support from far-right presidential candidate Marine Le Pen. Accordingly, across Europe as well as in the United States, defense officials and politicians are increasingly worried that they lack sufficient insight into the extent of far-right radicalization within military and police ranks, making this an urgent priority for more targeted research.

In any case, given its symbolic success, the January 6 insurrection will likely continue to influence and inspire far-right extremists in the years to come. Assessing the social media posts of the insurrection participants, Danielle Carrier, Ilana Krill, and Andrew Mines suggest,

> That members of violent extremist groups garnered a significant “self-efficacy boost” on 6 January from which to springboard future activity. Put another way, the individual and collective experiences of violent extremist group members on 6 January, as well as their perceptions of success in storming the U.S. Capitol, holds the potential to shape these members’ beliefs that they can successfully execute similar acts in the future.

However, they also note that some participants viewed the insurrection as a failure, with the Oath Keepers in particular experiencing some organizational fracturing. The authors suggest that such fracturing offers a potential off-ramp out of violent extremism.

Unfortunately, organizational fragmentation could also lead certain elements of the far-right to radicalize further and establish a more proactive militant plan of action and/or join proscribed far-right terrorist outfits. Scholars such as Colin P. Clarke, Bruce Hoffman, and Rasha al-Aqeedi have all warned that the terrorist landscape—including on the far-right—is likely over the coming years to become more fragmented and simultaneously...
cross-pollinated in terms of organizational structure and ideology.\textsuperscript{19} This position was echoed by FBI Director Christopher Wray in March, who warned that the United States faces a threat from “lone-wolf” terrorists or small cells motivated by a “mishmash” or “salad bar” of ideologies that can prove malleable and even mutually complimentary so long as the common denominator is a penchant for violence.\textsuperscript{20} This trend is still in its emergent stages, but already there have been several instances in which extremists have migrated from the far-right to the jihadist arena or even combined elements of both ideologies to justify violence.\textsuperscript{21}

In the specific context of platform usage, recent research has tracked how far-right extremists have had to adapt and innovate in response to the deplatforming efforts that followed January 6, moving to other platforms like Telegram—downloads of which increased 146 percent on the Apple Store following the insurrection\textsuperscript{22}—and Signal, which jumped from the 750\textsuperscript{th} most downloaded app on January 4 to the first most downloaded by January 12.\textsuperscript{23} Gab, which markets itself as a refuge for victims of “Big Tech,” enjoyed such an influx of users after January 6 that the application is now overburdened, creating glitches and delays.\textsuperscript{24} MeWe, a previously little-known app, likewise saw a dramatic increase in users after the Capitol insurrection.\textsuperscript{25} Given that large tech companies are likely to continue to face pressure to clamp down on far-right extremist speech moving forward, the ways in which extremists have responded to recent deplatformings hold important lessons for the future and, as such, are in need of further exploration.

Notably, it is not just far-right extremists that have been adapting and innovating online of late. Michael Krona notes that unofficial, supporter-driven media groups have accelerated their production of video propaganda on behalf of or aligned with the Islamic State of late.\textsuperscript{26} One of the “advantages” of this de facto decentralization of propaganda activities is that videos from unofficial outlets appear to be better able to remain live on mainstream platforms. Separately, nationalists in India have begun taking to a new Indian government-promoted domestic social media platform, Koo, which has garnered a reputation for hosting extreme ultranationalist voices and content (particularly since the eruption of China–India border clashes in summer 2020). Koo aligns its content moderation policies with the political and geopolitical interests of the government rather than any ostensibly apolitical terms of service or commitment to universal free speech and therefore presents a novel conundrum in the online extremism
Looking ahead, other nations are liable to develop similar forms of “sovereign” social media—for example, China is well ahead of the curve—reinforcing a trend in the Global South in which extremist rhetoric is intertwined with states’ geopolitical objectives and not just the ideological impulses of insurgent groups.

Three other emergent trends within the online space merit brief mention. The first is the co-optation of emergency events by far-right actors to sow division through disinformation. Timothy Graham observes that far-right extremists in Australia started a Twitter hashtag to claim that a series of wildfires were caused by Asian arsonists rather than climate change, a similar dynamic of which was seen with wildfires in the Pacific Northwest that far-right Twitter users blamed on Antifa. Second, members of the far-right are continuing to use “gamification” and “memification”—i.e., the use of games and meme interfaces to spread extremist content—in their day-to-day outreach. Ashley Mattheis for one notes that far-right extremists have begun using video game platforms to create avatars of far-right figures and digitally recreate live-streamed attacks like the 2019 Christchurch attack. Third, non-state extremist actors are eyeing emerging technologies to gain a competitive edge against state actors in the areas of funding and weaponry. During fighting between Israel and Hamas in June 2021, the Palestinian militant movement saw a surge in bitcoin donations from sympathizers around the globe. Meanwhile, in November 2020, a supporter of the Boogaloo Boys became one of the first extremists to be charged for mass-producing and selling gun components produced by 3D printer, which follows the first use of 3D-printed components in a terrorist attack in 2019.

Research Gaps and Priorities

It remains to be seen whether extremists who were banned from mainstream platforms in the aftermath of January 6 will remain offline or whether there will be something like a reversion to the status quo ante—the experience of Telegram takedowns against the far-right suggest the latter (see Section Three below), though other platforms may have more sustained success. With that in mind, it will be crucial for researchers to monitor whether there is any prolonged consolidation of far-right extremists on certain apps or whether such individuals will instead disperse to multiple apps and, taking the post-January 6 experience to heart, develop more elaborate contingency plans. Another crucial question in this regard, per Lydia Khalil’s work, is whether the lack of algorithmic recommendations on platforms such as Telegram is
offset in terms of recruitment and radicalization by the more interpersonal nature of engagements on the app. Any research in this regard would have significant relevance to policies surrounding deplatforming.

It will be similarly important for researchers to track the trajectories of the various far-right movements and ideologies that have gained ascendancy in the past few years, none more so than QAnon, given the degree to which its conspiracy theories have become mainstreamed. Practitioners and scholars alike would also benefit from research on the “salad bar” phenomenon identified by FBI Director Christopher Wray in March of this year.35 Any commonalities in terms of psychological traits or life experiences between individuals who have taken the “salad bar” approach would contribute to tailoring early-warning systems and P/CVE programming. It remains to be seen just how widespread the phenomenon actually is, however, which is why the immediate research priority should be to collate any existing data that may be relevant while remaining alert for signs of additional cases as they may arise.

Lastly, research into the role of technological innovations as enablers of extremism should be prioritized. As cryptocurrencies gain more mainstream acceptance, their illicit use may increase too, a trend that research from Alexis Henshaw has already identified.36 Similarly, as 3D printing becomes more accessible, researchers would do well to investigate what factors influence (and limit) an extremists’ decision to use 3D-printed weapons or components as opposed to acquiring such devices through other means (especially given the costs and limitations of 3D printing).
Section Two

Messaging and Outreach

Research shows that the social and geopolitical tumult of the past year has exacerbated popular discontent in many societies, expanding the pool of potential recruits into violent extremist organizations. Extremists have tailored their outreach and messaging accordingly.

On Telegram, the influx of new users from Facebook, Twitter, Parler, and the like offers new potential recruits for those extremists already entrenched within the platform. However, the nature and tone of material in far-right Telegram chats is far more extreme than what has traditionally been espoused by far-right activists on other platforms. As Canadian scholar Amarnath Amarasingam noted in the immediate aftermath of the de-platformings that followed January 6, “[Telegram is] not simply pro-Trump content, mildly complaining about election fraud. Instead, it’s openly anti-Semitic, violent, bomb making materials and so on. People coming to Telegram may be in for a surprise in that sense.”

This has not been lost on far-right Telegram users, who have proactively sought to tailor their messages to the uninitiated, carefully laying the groundwork to “redpill” ordinary Trump supporters (to use the parlance of many far-right extremists). Surveying neo-Nazi and white supremacist Telegram chats, Meili Criezis finds that extremists have been circulating advice on how to “redpill” “normie” (i.e. non-extremist) Trump supporters, including by building one-on-one relationships in private chats, gradually stoking a sense of disaffection with Trump and mainstream conservatism, then introducing more extreme ideological messaging.

Among other things, Criezis notes,

> These manipulative messages are designed to elicit strong emotions in their targets ranging from fear, anger, and hope – among an array of others – while simultaneously offering a sense of belonging in a “new” community, i.e. hardcore white supremacist groups and ideologies. Perhaps most importantly, the critical threshold they want Trump supporters to cross is... regarding the “work for a white well-being.”

However, far-right extremists in the United States must also contend with a significant inconvenient truth: the January 6 insurrection failed to prevent...
Joseph Biden from becoming president. This reality has required a lot of improvised and often incoherent narrative shifting. Many Trump supporters on Gab quickly began claiming that the Capitol assault was a “false flag” conducted by left-wing activists, a claim which (according to one poll) half of Republican voters believe. This false flag claim may have actually helped dissuade members from taking part in planned demonstrations in the subsequent days leading up to and on inauguration day.

For supporters of QAnon, the failure is theoretically even greater since the outlandish predictions of the eponymous Q—that Trump would be reinstated and arrest numerous Democratic party leaders, and so on—never came to pass. However, many (if not most) QAnon supporters seem to not be dissuaded, either pushing back the date of the anticipated events, claiming partial victory (such as gaining publicity), or appealing to spiritual authorities (a path that is incidentally well-trodden by jihadist extremists). This has led researchers like Brody McDonald to conclude that not only is the movement likely to survive, but that,

QAnon supporters are beginning to feel led to take matters into their own hands after seeing that they cannot expect political or military leaders to implement their vision... the failed predictions of the past may well spur some QAnon supporters to take direct action and fuel a new, more dangerous, stage in the development of the movement.

The COVID-19 pandemic, and more specifically anti-lockdown sentiment, has also become a focal point of extremist messaging over the past year or so. Argentino for one finds that some violent far-right organizations and movements such as the Boogaloo Boys have adopted conspiracies from QAnon related to the lockdowns, which they see as evidence of a “deep state” stifling citizens’ liberties. This shows a degree of ideological diffusion across the American far-right. Argentino also notes that the pandemic has created factors that increase potential recruitment for violent extremist organizations such as increasing social isolation and economic hardship—factors that might outlast the pandemic. While jihadist groups like al-Qa’ida and the Islamic State have generally been more ambiguous in relation to the COVID-19 pandemic, the same cannot be said for their supporters, who continually refer to the pandemic as a punishment from God targeted at their irreligious enemies.

Another key flashpoint for COVID-19 messaging relates to anti-lockdown
sentiment. Germany has emerged as one of the biggest centers of anti-lockdown sentiment in Europe—a symptom, in part, of the growth of the far-right in the country in recent years. Jakob Guhl finds that, specifically during the pandemic, Germany’s far-right has expanded its online reach far more than either the far-left or Islamist movement. Its constituent parts have done so by tapping into the loss of control that ordinary people experienced in the wake of public health-related restrictions, a discourse trend seen elsewhere too. In a similar vein, Chamin Herath et al. have found that the rhetoric of the far-right opposition party Alternative for Germany (AfD) has shifted dramatically from the early days of the pandemic when it criticized the German government for its slow response, with the party now mainstreaming disinformation and conspiracy theories that link lockdown concerns to longstanding preoccupations around immigration and the influence of a transnational elite. Again, this trend is by no means confined to Germany and, as states in Europe and North America in particular progress with their respective vaccination campaign, it will be crucial to see how the far-right responds and adapts.

Besides lockdowns, another focal point of extremist COVID-19 rhetoric is 5G, something that has resulted in real-world violence, including the destruction or sabotage of 5G towers. Extremists and conspiracists of all stripes have long advocated sabotaging or destroying critical infrastructure as a means of hastening societal collapse. Since January 2020, accelerationists in particular have found a voice in anti-5G communities, a voice that has grown beyond the fringes of the anarchist or far-right as conspiracy theorists (starting with an obscure Belgian doctor) have linked 5G signals to COVID-19. Since then, there have been dozens if not hundreds of attacks against 5G infrastructure across Europe and North America. Michael Loadenthal notes that many of these incidents seem to be the work of COVID-19 conspiracists rather than accelerationists, though far-right extremists frequently cheer such incidents nonetheless.

Looking forward, it seems unlikely that 5G-related conspiracies will lose much traction as COVID-19 is suppressed in Western societies. Already, several prominent conspiracy theorists have linked the technology to a host of other ailments such as cancer and infertility. Relatedly, eco-fascism, which often contains neo-Luddite currents, is on the rise, attempting to channel concerns about climate change to far-right ends and raising the possibility of increasing attacks on critical infrastructure conducted in the name of right-wing environmentalism. Given that climate change is likely...
to become more disruptive and undeniable in the coming years, Friederike Wegener warns that eco-fascism is poised to become more relevant to the far-right.  

Another at least partial impact of the COVID-19 pandemic is that China and Chinese people are emerging as new targets of extremist ire among both far-right activists and jihadists, though the picture is complex in each case. Indeed, it is not just suspicions around the origins of COVID-19 driving this trend: China’s increasingly hostile relationships with many Western countries have contributed to a resurgence of Sinophobia (which generally have a long history of anti-Asian xenophobia), and China’s abuses against its Uyghur Muslim population—which arguably constitute genocide—have prompted an outcry from many Muslim communities (though crucially not Muslim governments).

On the Islamist side of the equation, China has by no means supplanted the United States as the “Great Satan,” but there are signs that jihadists are directing more of their attention at the country, a gradual shift several years in the making that could be accelerated by COVID-19. The Islamic State for one ascribed the COVID-19 pandemic to divine punishment for China’s treatment of its Muslims. Jihadist propagandists have also accused China of pursuing anti-Muslim policies abroad, from its support for the Myanmar government (which is persecuting Rohingya Muslims) to its Belt and Road activities in central Asia and the Middle East. Over the past year, jihadists have attacked Chinese interests from Mozambique to Pakistan, as Lucas Webber notes, though this does not itself suggest a coordinated anti-China campaign across countries and groups. For that matter, jihadist attacks within China are quite rare, compared to (say) in Africa, where Islamic State affiliates in particular have consolidated over the last year or so. Nonetheless, as China’s economic (and in some instances military) presence looks set to increase across Eurasia and Africa in the near future—and as Beijing continues to oppress Muslims at home—jihadists may grow more tempted to strike Chinese interests, so this is an issue worth watching closely.

In Western societies (including many European countries), anti-Chinese and anti-Asian sentiment has increased notably since early 2020, with many accusing President Trump himself in the early days of the pandemic of stoking xenophobia by using terms such as “China Virus” and “Kung Flu.” Kaz Ross notes that in Australia, a combination of the pandemic and an
escalating trade war with Beijing have led China and the Chinese Communist Party (CCP) to become a rallying point for a diverse set of political groups, including the far-right, which has adopted more anti-China rhetoric as part of its pandemic-era recruitment strategy.\textsuperscript{56}

**Research Gaps and Priorities**

In the context of anti-East Asian bigotry, there are several important knowledge gaps that merit further research. As Meili Criezis notes in her examination of far-right responses to the March 2021 shooting of six Asian women in Atlanta, Georgia,

> There remains a significant gap in comprehending how white supremacists and the far-right express anti-East Asian sentiments and/or promote certain narratives about East Asians as a means to target other racial minorities.\textsuperscript{57}

Given that in certain white supremacist circles, East Asians are seen as preferable to other minorities, with some even considering East Asians “honorary Aryans,”\textsuperscript{58} it will be important for researchers to distinguish how different sub-sets of the far-right react to China’s geopolitical behavior. For that matter, it is unclear what role, if any, specifically violent far-right extremists have had in contributing to the spike in anti-Asian bigotry.

Additionally, more psychological assessments of the role of conspiracies in motivating individual violent behavior would be a welcome contribution. As William Allchorn notes,

> The role of conspiratorial narratives in [right-wing lone actors] trajectories towards violence is something that has been under-explored and under-utilised. Previous analyses have looked at group- or campaign-based expressions of conspiracy theories... rather than individual risk factors.\textsuperscript{59}

Relatedly, researchers should examine the impact that platform migration has had on far-right radicalization—in other words, whether far-right extremists have had much success “redpilling” the “normie” Trump supporters who found refuge in Telegram after January 6.

With regards to jihadism, the academic and policy communities would
benefit from more comprehensive, quantitative data on jihadist propaganda, rhetoric, and attacks as they pertain to COVID-19 as well as China and Chinese interests. Jihadists may be speaking about China more than they previously have, but without any comparison to the relative volume of rhetoric and attacks targeted against local government or Western interests, it is impossible to gauge the extent to which jihadists see China as an adversary to prioritize.

Section Three

Preventing Terrorist Use of the Internet (PTUI)

Over the course of the last six months, governments, corporations, and researchers alike have increasingly been discussing how best to leverage tools such as big data, social media, and artificial intelligence (AI)-driven predictive technologies (among others) to combat and prevent terrorism and violent extremism. While these tools hold much potential, each tool also faces its own limitations and entails its own challenges.

Focusing on predictive visualization technologies, Shiri Krebs warns of several distinct problems, including an accountability gap in which counterterrorism operators can blame faulty technology for their own errors. Given the greater role predictive visualization technologies are likely to play in counterterrorism moving forward, Krebs recommends improving transparency surrounding the data methodologies behind such platforms. Similarly, while some researchers have spoken of the potential for big data and machine learning to transform counterterrorism, others are more skeptical. H.M. Verhelst, A.W. Stannat, and G. Mecacci for example argue that terrorist attacks, particularly so-called “lone-wolf” attacks, leave irregular and isolated digital footprints that make them difficult to predict. The authors also contend that machine learning-driven surveillance risks blurring the already nebulous line between the collection of metadata and personal data.

New research suggests that there is no silver bullet when it comes to disrupting extremist communications. Examining data from Pakistan, Fatima Mustafa finds that terrorist attacks decline on the day of a government-imposed cellular shutdown but increase the following day. Amarnath Amarasingam and Rukshana Rizwie similarly argue that social media shutdowns in Sri
Lanka have done nothing to limit the spread of misinformation—the Sri Lankan government’s primary justification for employing the tactic—given that ordinary citizens respond by simply switching to virtual private networks (VPNs). On the other hand, Amarasingam, Shiraz Maher, and Charlie Winter are more optimistic when it comes to the potential for disrupting jihadists on Telegram. In their study of Europol’s 2019 “Action Day,” the authors find that Telegram takedowns are effective when coordinated, sustained, and coupled with offline counterterrorism efforts. Héni Nsaibia and Rida Lyammouri are more skeptical, however, noting that jihadist channels temporarily moved to other messaging platforms before eventually returning to Telegram, noting that Telegram failed to continue cracking down on channels in the absence of continued pressure from Europol or similar authorities.

In any event, far-right and jihadist presences on Telegram are not analogous, limiting the applicability of the Europol take downs for far-right extremist content. While Telegram made efforts to ban many popular far-right chats after January 6, most users were able to reconstitute in new chats—often with near-identical names—in very short order. This is not surprising, as Maura Conway has recently explained that de-platforming the far-right is much more difficult than de-platforming jihadists. For one, the former is a dynamic and fast-changing scene characterized by loose networks rather than formal organizations (the latter being easier to target). Far-right rhetoric is also more mainstreamed than jihadist rhetoric in the West, and is thus also more profitable for social media companies.

Marc-André Argentino similarly argues that existing counterterrorism toolkits and threat assessments are unprepared for the multiplicity of platforms on which extremists radicalize, recruit, mobilize, and coordinate. Indeed, previous de-platforming efforts could conceivably backfire (although there is no evidence one way or the other at present) as Argentino ominously notes that the number of new Telegram users exposed to far-right content in the aftermath of January 6 dwarfs that of Islamic State sympathizers on the app. Additionally, Eviane Leidig argues that non-Western far-right movements pose unique and underappreciated challenges for PTUI that tech companies must better appreciate.

This is not to suggest that there is no opportunity for innovation in the PTUI space. Several governments have begun to pass more proactive legislation in this regard. Australia recently introduced new laws to disrupt terrorist
activity on the dark web.\textsuperscript{71} Separately, a bill under deliberation in New Zealand’s parliament would criminalize the live streaming of “objectionable” content such as a terrorist attack,\textsuperscript{72} while Singapore recently passed a law criminalizing “unauthorised possession of blueprints” for “the manufacture of a gun or a major part of a gun on a 3D printer.”\textsuperscript{73} Of course, legislation aimed at PTUI can overreach and violate civil liberties, as it arguably has in France, for example.\textsuperscript{74} With this in mind, Alastair Reed, Adam Henschke, and Kateira Aryaeinejad have recommended several elements that authorities should incorporate into content moderation frameworks moving forward.\textsuperscript{75}

Researchers have also identified new ways in which technology can potentially assist P/CVE efforts. For example, Linda Schlegel and Teo Kai Xiang each argue that “gamification” and game-based learning should not be the sole domain of extremists but can instead be turned into an effective P/CVE tool.\textsuperscript{76} And in Indonesia, the COVID-19 pandemic prompted prison deradicalization programs to shift to videoconferencing apps. While this arrangement was not without shortcomings, Cameron Sumpter concludes that virtual programs offer a useful supplement to in-person engagements.\textsuperscript{77}

One of the primary challenges facing researchers and practitioners working in the PTUI space is a legal and technical one: The Global Internet Forum to Counter Terrorism (GIFCT) offers tech companies a shared database of specifically “tagged” terrorist content to remove—but this database, far from being exhaustive, is based solely on the U.N. Security Council’s consolidated sanctions list. Brett Raffish argues that the U.N. list is not geographically balanced (skewing towards the Middle East and Africa and overlooking other crucial regions), not based on universally accepted definitions of terrorism and violent extremism, and not maintained and updated in a timely manner.\textsuperscript{78} Raffish consequently suggests that GIFCT consider maintaining its own list moving forward.\textsuperscript{79} Researchers would do well to further interrogate this line of reasoning.

There is also a need to further explore the relationship between an individual’s behavior online and their propensity for violence offline. Ryan Scrivens et al. offer a valuable (and perhaps counterintuitive) assessment in this regard, noting that violent far-right extremists examined in their study posted online significantly less than their non-violent extremist counterparts.\textsuperscript{80} This matter merits further study given its policy relevance.
Conclusion

After nearly two decades of focusing almost exclusively on the threat of jihadist terrorism, policymakers, researchers, and practitioners are today confronted with a fast-evolving and ascendant far-right violent extremist threat, something that has borne out in academic and policy research circles over the last six months. The far-right movement (if it is even coherent enough to be considered one) is diffuse, fractured, highly adaptable, and frequently benefits from disinformation and polarization within the mainstream of Western politics. At the same time, jihadism remains a versatile threat, albeit one that is much more pronounced in Muslim-majority countries than in Western societies. Whatever their ideology, violent extremists are employing technology and online spaces to advance deadly and destructive aims more than ever today, increasingly demonstrating a degree of cross-ideological learning and inspiration.81

Researchers and practitioners must be alert to the emerging trends and research priorities laid out in this white paper moving forward. Rarely is there a silver bullet in the work of counterterrorism and P/CVE, as underscored by the mixed record of de-platforming described in Section Three. Nonetheless, through creative, forward-looking, and (perhaps most importantly) collaborative efforts, the tech, academic, government, and P/CVE and counterterrorism communities can stay one step ahead of violent extremists and other malevolent actors in the contests of narratives and innovation.
Endnotes

3 For more data on federal cases related to the Capitol Hill siege, refer to the Program on Extremism at George Washington University.
6 Data obtained from the Program on Extremism.
18 Carrier, Krill, and Mines, “I will never forget this.”

25 Criezis and Galloway, “From MAGA to the Fringe.”


36 De Vynck and Nakashima, “Far-right groups move online conversations from social media.”

52 Webber, “China’s Policies.”
58 Criezis, “Rhetoric of Hate.”

Argentino, “Extremism Unmasked.”

Leidig, “Far-Right in the Global South.”


For more, see Barnett, Maher, and Winter, Innovation, Creativity, and the Interplay Between Far-Right and Islamist Extremism.
To learn more about the Global Internet Forum to Counter Terrorism (GIFCT), please visit our website or email outreach@gifct.org.