United States Senate Committee on

Homeland Security & Governmental Affairs

U.S. Senator Gary Peters | Chairman

The Rising Threat of Domestic Terrorism

A Review of the Federal Response to Domestic Terrorism and the Spread of Extremist Content on Social Media

A HSGAC Majority Staff Report

November 2022

I. EXECUTIVE SUMMARY

Over the past two decades, acts of domestic terrorism have dramatically increased. National security agencies now identify domestic terrorism as the most persistent and lethal terrorist threat to the homeland. This increase in domestic terror attacks has been predominantly perpetrated by white supremacist and anti-government extremist individuals and groups. It is clear that the federal government is not adequately addressing this growing threat, but without better data, it is difficult to evaluate whether federal agencies are appropriately allocating resources and setting priorities. Although outside researchers have reported on trends relating to domestic terrorism, the federal government has not systematically tracked and reported this data itself, despite being required to do so by law. Social media platforms have played an increasing role in the spread of extremist content that translates into real world violence, due in part to business models that incentivize user engagement over safety.

This report is a culmination of three years of investigation by the Majority Committee staff for U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee (HSGAC) into domestic terrorism and the federal response. This report focuses on the rise in domestic terrorism, the federal response, the allocation of federal resources to addressing domestic terrorism, and the role of social media companies in the proliferation of extremist content. The Committee held eight hearings over the last three years on the rising domestic terrorism threat. As a part of this investigation, Chairman Peters sent document and information request letters to the Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, Meta (formerly known as Facebook), Twitter, YouTube, and TikTok. The Committee also held briefings and interviews with the agencies and companies. Committee staff reviewed over 2,000 key documents obtained from federal agencies and social media companies in response to the Committee's requests for information.

* * * * *

In the aftermath of the terrorist attacks on September 11, 2001, Congress restructured the federal government to focus on the threat posed by international terrorists. This included the creation of the Department of Homeland Security (DHS) and an early version of what would later become the Office of Intelligence and Analysis (I&A), an expansion of investigative authority within the Department of Justice (DOJ), and creation of the Terrorist Threat Intelligence Center (TTIC), the precursor to the National Counterterrorism Center (NCTC). However, in the more than twenty years since the federal government shifted its focus predominantly toward international terrorism, attacks from domestic terrorists have surged. According to a 2021 Center for Strategic and International Studies study, there were 110 domestic terrorist plots and attacks in 2020 alone, a 244 percent increase from 2019 and a 275 percent increase from 2017. According to the Anti-Defamation League, from 2012 to 2021, domestic extremists have been responsible for 443 deaths, with over 50 percent of the deaths caused by white supremacists.

Since 2019, DHS and the Federal Bureau of Investigation (FBI) have repeatedly identified domestic terrorism, in particular white supremacist violence, as the most persistent and lethal terrorist threat to the homeland, including in multiple threat alerts provided to Congress

and law enforcement agencies across the country. Despite this acknowledgement and multiple analyses, plans, and National Strategies across multiple Administrations, this investigation found that the federal government has continued to allocate resources disproportionately aligned to international terrorist threats over domestic terrorist threats.

For instance, the federal government still fails to comprehensively track and report data on domestic terrorism despite a requirement from Congress to do so. Under a provision Senator Peters helped secure, the fiscal year 2020 National Defense Authorization Act requires DHS, DOJ, and NCTC to issue an annual *Strategic Intelligence* report to provide a strategic intelligence assessment and data on domestic terrorism. The agencies provided the first *Strategic Intelligence* report nearly a year after the statutory deadline and omitted significant amounts of required information, including comprehensive data on domestic terrorism incidents and agencies' staffing and resource allocation to address the threat. The 2021 *Strategic Intelligence* report, in its intelligence assessments, identified domestic violent extremists as the most persistent and lethal terrorist threat to the homeland. However, DHS provided little information on its intelligence processes, DHS and FBI provided little to no data on domestic terrorism, and no agency provided recommendations to Congress for how to assist in addressing domestic terrorism. The agencies provided their 2022 *Strategic Intelligence* report in October 2022, nearly five months late. While this report provided more information on agency actions and some data, it still failed to comply with all statutory requirements.

The federal government's current definitions and categorizations of domestic terrorism also create challenges. FBI and DHS have different definitions for "domestic terrorism," which could lead to the two agencies categorizing the same event as different types of terrorism. Law enforcement and national security agencies have greater surveillance, investigative, and prosecutorial tools and resources available to respond to terrorist acts labeled as "international" rather than "domestic." These differences often lead to disparate treatment of immigrant and U.S. minority populations and inconsistent investigations of terrorist attacks, including whether or not to categorize an attack as terrorism. Federal agencies have trouble distinguishing between what is "domestic" and what is "international" due to the increasingly global nature of extremism. This investigation also determined that the current definitions and categorizations used by FBI obscure the threat posed by white supremacist violence.

The expansion of social media has also led to increased recruitment, dissemination, and coordination of domestic terrorist and extremist related activities. According to a National Consortium for the Study of Terrorism and Responses on Terrorism study, in 2016 alone, social media played a role in the radicalization process of perpetrators in over 90 percent of extremist plots or activities in the United States. Domestic terrorist groups use a range of social media platforms to recruit, communicate, train, and mobilize members, leading to the rapid expansion of potential threats. Extremist content proliferates on these platforms, despite rules against such content and moderation measures designed to remove the content.

The First Amendment, the Privacy Act of 1974, Executive Order 1233, and agency specific guidance govern and rightfully limit how federal agencies use social media for law enforcement and intelligence purposes. Federal agencies are permitted to use social media within the bounds of civil rights and civil liberty restraints, but oversight entities have found that

the federal government has not adequately utilized tools and resources to address domestic terrorist threats on social media.

Social media companies often point to the amount of violative content they remove from their platforms as a sign of their actions to address extremism. While actions taken to remove violative content are commendable, the sheer amount of content companies have to remove shows just how pervasive such content is on these platforms. Content moderation efforts alone will never be sufficient to address the problem. This investigation examined four large social media companies and found that terrorist and extremist content permeates social media platforms in part because these platforms' business models are designed to maximize user engagement, which has the effect of promoting increasingly extreme content. Major social media companies that the Committee examined are aware of this problem, but absent incentives or regulations requiring that they do otherwise, these companies have continued to prioritize growth and engagement and have not taken sufficient action to address this threat.

- **Meta** has been aware of the harm that its products cause for years. Internal documents provided by a Meta whistleblower show that Meta's recommendation features are designed to provide users with content they are most likely to engage with, such as posts that users may comment on or groups users may join. These recommendations often drive the spread of harmful and violative content, according to internal Meta research and external researchers. Despite this awareness, Meta has chosen in some instances to not make changes to its features and products that would alter what content is prioritized for viewers (on the front end), and instead the company addresses what it terms "trust and safety" issues primarily by taking down violative content (on the back end) after it has already appeared and spread on its platforms, sometimes to millions of users and in some cases after years of remaining on the platform.

- **TikTok** also uses recommendation features based on user engagement, in particular the amount of time spent consuming individual pieces of content. Outside research has shown that TikTok's algorithm pushes users towards more extreme content because that is the content users engage with the most. Despite these concerns, in an interview with Committee staff, TikTok's Chief Operating Officer (COO) explained that she did not believe the company had conducted research into whether the company's algorithms promote extreme content. TikTok's COO also told Committee staff that while employees are compensated based on their performance, there is no measure of trust and safety that directly affects compensation.

- **Twitter** generates a list of accounts it recommends users follow based on the user's engagement with similar accounts and topics, creating a "rabbit hole" effect that can promote conspiracy theories and extreme content. Twitter was central to the spread of QAnon conspiracy theories and the "Pizzagate" conspiracy that falsely alleged that public officials were linked to a human trafficking and child sex ring out of a pizzeria in Washington, D.C. While Twitter has yet to conduct certain research (such as the underlying reasons why its algorithms give greater amplification to content from what it defined as right-wing politicians than left-wing politicians), outside research has found

that the Taliban and white supremacists utilized Twitter's Spaces feature to spread extremist content to hundreds of users.

- Over 70 percent of viewing time on **YouTube** is generated by the platform's recommendation system, which is based on users' engagement on the platform and activity on Google. Researchers have long criticized YouTube for the platform's features that push users towards extreme content or down "rabbit holes" of content. Research conducted by MIT's Technology Review found that "users consistently migrate from milder to more extreme content" on YouTube. Despite this knowledge, in an interview with Committee staff, YouTube's Chief Product Officer could not point to internal research done to evaluate whether the platform recommends extreme content.

This report finds that the federal government – specifically FBI and DHS – has failed to systematically track and report data on domestic terrorism as required by federal law, has not appropriately allocated its resources to match the current threat, and has not aligned its definitions to make its investigations consistent and its actions proportional to the threat of domestic terrorism. This report also finds that social media companies have failed to meaningfully address the growing presence of extremism on their platforms. These companies' business models are based on maximizing user engagement, growth, and profits, which incentivizes increasingly extreme content – and absent new incentives or regulation, extremist content will continue to proliferate and companies' moderation practices will continue to be inadequate to stop its spread.

II. FINDINGS OF FACT AND RECOMMENDATIONS

FINDINGS OF FACT

Domestic Terrorism Threat

1. Domestic terrorism has been increasing over the last several years, surpassing international terrorism as the most significant terrorism threat to the United States. The threat from domestic violent extremism has increased significantly since 2015 – especially among white supremacists, anti-government extremists, and militia violent extremists – and federal officials predict that the threat will persist. Domestic terrorists have committed an increasing number of nonlethal acts as well as fatal attacks, with more deaths in recent years caused by domestic terrorists than by foreign terrorist organizations.

2. White supremacist extremists pose the primary threat among all domestic violent extremists. The Department of Homeland Security (DHS) provided the Committee with data showing white supremacists were responsible for 51 out of 169 domestic terrorist attacks and plots from 2010 through 2021, the highest number among domestic terrorist ideologies.

3. Domestic terrorism attacks have been plotted using, and inspired by, content on social media. Social media platforms have increasingly been used by domestic terrorist organizations, including the Proud Boys and Oath Keepers, to promote violent ideologies, disseminate hateful messages, radicalize individuals, and mobilize individuals towards violence. For example, the January 6th attack on the U.S. Capitol was planned and discussed on multiple social media platforms, and the perpetrator of the May 2022 shooting in Buffalo, New York, was radicalized by racist and violent content on social media such as the Great Replacement Theory, and the video of the shooting was reposted on Facebook, Instagram, and Twitter.

Federal Agencies

4. Since the September 11, 2001, terrorist attacks, additional counterterrorism authorities and resources for the federal government have been focused primarily on international terrorist threats. Changes to federal law in the wake of 9/11 gave federal agencies more surveillance and investigative powers, which focused the government's efforts on international threats that were previously missed. While these authorities have resulted in critical successes in preventing attacks in multiple locations across the U.S., they have also led to abuses of civil liberties and a disproportionate focus on international terrorist threats over domestic terrorist threats.

5. In 2019, DHS publicly acknowledged white supremacist violence as a major threat to national security for the first time, despite being aware internally of the severity of the threat for 10 years. In a 2019 report, DHS acknowledged that white supremacist violence "is one of the most potent forces driving domestic terrorism." This was DHS's first

public acknowledgement of the severity of the threat, despite the Department discussing the threat in its non-public 2009 Intelligence Assessment entitled *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment*—which, while accurate, was ultimately rescinded by DHS due to political pressure. DHS also previously issued a non-public Joint Intelligence Bulletin with the Department of Justice (DOJ) in 2017 entitled *White Supremacist Extremism Poses Persistent Threat of Legal Violence*.

6. In 2021, the Biden Administration released the first-ever *National Strategy for Countering Domestic Terrorism*, detailing the Administration's overarching approach to addressing the evolving domestic terrorism threat. As part of its implementation of the *Strategy*, DHS designated combating domestic violent extremism as a "National Priority Area" within its Homeland Security Grant Program for the first time. Further, the DHS Secretary established a dedicated domestic terrorism branch within the Department's Office of Intelligence & Analysis (I&A).

7. DHS and FBI have not fully complied with requirements in federal law to collect and report data on domestic terrorist attacks. Both agencies are required by the 2020 National Defense Authorization Act to submit to Congress an annual report detailing each agency's efforts and resources dedicated to addressing domestic terrorism, annual assessments of the threat landscape, and data on domestic terrorism. DHS and FBI submitted the first *Strategic Intelligence Assessment and Data on Domestic Terrorism* almost a year late and did not provide the required information and data on domestic terrorism incidents and agencies' staffing and resource allocation, and the first annual update was nearly five months late and still did not include all required data.

8. FBI in recent years has changed how it categorizes domestic terrorism ideologies. In 2017, FBI created a new category of domestic terrorism ideology called "Black Identity Extremists," but has since terminated the use of this category. By 2019, FBI combined all forms of racially motivated extremism, including the pre-existing category of "White Supremacist Violence," into one category called "Racially Motivated Violent Extremists." This change obscures the full scope of white supremacist terrorist attacks, and it has prevented the federal government from accurately measuring domestic terrorism threats.

9. Agencies can and do monitor social media for threats of domestic terrorism, with certain limitations. Federal agencies are allowed to, and do, use social media when addressing domestic terrorism. However, they are limited in their use by the First Amendment, the Privacy Act of 1974, Executive Order 12333, and internal agency policy and guidance documents. Agencies have been slow to adapt to the open planning of extremist violence online, leading to incomplete threat assessments.

Social Media Companies

10. Extremist content continues to proliferate on social media platforms, at least partially driven by the companies' own business models, which prioritize engagement, profits, and growth over safety. Social media platforms focus their products and features on keeping users engaged, which leads the platforms to recommend increasingly extreme content.

11. In response to accusations that their platforms amplify extreme content, social media companies emphasize the volume of content they remove, rather than address why their platforms allow the proliferation of harmful content in the first place. Data provided to the Committee by social media companies about the volume of extremist and other violative content on their platforms helps illustrate the problem. Meta banned over 250 white supremacist groups and 890 militarized social movements through October 2021, Twitter took down over 1.8 million accounts for violating guidelines against the promotion of terrorism between 2015 and 2021, and YouTube removed 431,000 videos that promoted violent extremism in the second quarter of 2021 alone.

RECOMMENDATIONS

Federal Agencies

1. Reassess the federal government's counterterrorism efforts. Congress should require a whole-of-government review of federal counterterrorism efforts, including whether current post-9/11 structures, resources, intelligence, and enforcement efforts are sufficiently aligned to effectively address the current terrorism threat. This should include assessing relevant federal agencies' counterterrorism policies and procedures; identifying weaknesses, inefficiencies, and duplications in counterterrorism efforts; and ensuring international and domestic terrorism threats are properly defined and prioritized appropriately, as the lines that previously defined domestic and international terrorism are increasingly blurred.

2. Create a Counterterrorism Coordinator within DHS. Congress should create a Counterterrorism Coordinator within DHS to oversee counterterrorism strategy and operations within DHS. Congress should require this position to regularly report to Congress on DHS counterterrorism efforts and how DHS allocates resources based on the terrorism threat landscape.

3. Establish measurable standards for assessing agency counterterrorism efforts. Congress should require DHS and FBI to establish clear and quantifiable criteria to regularly report on the threat landscape and to measure implementation of frameworks, strategies, and initiatives to address domestic terrorism. Congress should further require the agencies to inform Congress on the results of those assessments, criteria employed to allocate and shift resources as threats evolve, and whether and how such actions address current threats, including whether changes are required where counterterrorism efforts are not successful.

4. Create accountability for complying with data reporting requirements. Congress should consider a range of accountability mechanisms for agencies that fail to provide information, data, and reports on the domestic terrorism threat as required under the FY 2020 National Defense Authorization Act (NDAA), including requiring DHS and FBI to certify to Congress compliance with reporting requirements and to identify any failures in reporting.

5. Develop a standardized system for reporting domestic terrorism data. DOJ and FBI should develop a system to consistently report internally and to Congress on all domestic terrorism investigations, arrests, and prosecutions, regardless of which part of the federal government pursues the case.

6. Create standardized domestic terrorism categories. DOJ and FBI should ensure their domestic terrorism categories are relevant and useful for defining the threat, collecting data, and planning and implementing strategies and actions to counter the threat. Congress should require FBI to report to Congress when making changes to the categories.

7. Clarify and improve federal agency guidelines on the use of social media while respecting individuals' constitutional rights. DHS, DOJ, and FBI should improve and clarify their guidance on how employees collect and use social media information. FBI should also provide guidance on the effective and consistent use of its third-party software tool for analyzing social media posts. All guidance must comply with protections in federal law and constitutional limitations, including the First, Fourth, and Fourteenth Amendments, and the agencies should be transparent about what data they use regarding social media.

8. Improve the effectiveness of relationships with social media companies regarding domestic extremist content. DHS and FBI should improve avenues of communication with social media companies for the companies to more effectively and consistently share threats coming from domestic extremist content found on their platforms. These avenues of communication and relationships must be appropriate under constitutional restrictions, federal law, and agency guidelines.

Social Media Companies

9. Create accountability for social media companies to prioritize safety on their platforms. Congress and regulators should create accountability mechanisms for social media companies to prioritize safety in the development of their products and features, and consider removing current protections in law that allow companies, without meaningful consequences, to continue to prioritize engagement on their platforms even if that results in knowingly promoting extreme content.

10. Conduct research on platform design. Social media companies should be required to conduct – and report to appropriate regulatory bodies – research on their platforms to understand the impacts of platform design and recommendation algorithms on the

amplification of violative or extreme content on their platforms, including before launching new features or products.

11. Establish transparency mechanisms to allow external research. Congress should codify transparency requirements for social media companies to provide outside researchers, including academic researchers, nonprofit organizations, and journalists, access to raw data and metadata, including content on social media platforms, advertisements, and metrics around algorithmic processes. Congress should mandate that this access protect user privacy and proprietary information.

12. Establish trust and safety as prioritized metrics. Congress should require large social media companies to quantify and release specific metrics on trust and safety, including detailed metrics on the levels of extremist, violent, and other violative content on their platforms and the distribution of users who see that content, including if certain individuals or communities see a disproportionate amount of harmful content. Congress should mandate that platforms publicly release the prioritized metrics for their products including those used in A/B testing and in determining employee compensation.