NATIONAL COUNTERTERRORISM CENTER

DOMESTIC TERRORISM

CONFERENCE REPORT

JANUARY 2020

The National Counterterrorism Center, together with FBI and DHS, held a conference from 23 to 24 September 2019 to examine the US Government's approach to confronting the threat of domestic terrorism (DT) and to inform future DT policy. The conference convened stakeholders from academia, the private sector, and across the Federal Government, including intelligence and Non-Title 50 agencies, to explore four themes: *Terminology, Authorities, Operations, and Expanding Partnerships.* This report is intended to capture the content of the conversations held at the conference, and does not represent the views of any particular department, agency, panelist, or participant.

Key Takeaways

The following themes emerged from all four sessions:

> "This conference is really a workshop, a call to action, and we are here to determine how to better inform policymaking on DT and determine the 'so what' and the way ahead." -Acting DNI, Joseph Maguire

- Although the threat from DT is not new, radicalization and communication of DT actors has evolved in recent years and remains potent.
- Because an increasingly larger part of the activity related to DT occurs online and is constitutionally protected, increased collaboration among partners—including academia, NGOs, and state, local, and federal law enforcement—will help combat this evolving threat.
- Most conference participants agreed that current federal criminal statutes do not include a distinct law criminalizing acts of DT, leaving prosecutors to rely on existing criminal statutes to address DT-related offenses, indicating a need for legislative review.
- Most conference participants agreed that a domestic terrorist organization designation, similar to the current process for designating foreign terrorist organizations, could be useful in combating DT; however, DT actors in the Homeland and abroad are aware of the activities that merit designation and adjust accordingly to avoid prosecution.
- Noting the legal challenges to enacting a domestic terrorist organization designation, there was support for using the foreign terrorist designation process to proscribe DT analogues overseas.
- Legal mechanisms available to some foreign partners, e.g., to ban DT groups, are at odds with US civil liberties. Creating a DT designation in the United States could be perceived as government overreach and/or unconstitutional.
- Conference participants noted the significance of the role of terminology in DT, as definitions laid out in statute are used to determine the allocation of tools and resources to departments and agencies. Using terminology solely derived from authorities can be restrictive, proscribing which departments/agencies participate in DT efforts, and lacks the flexibility to be useful for all US Government DT efforts. This impacts how the US Government responds to DT threats, requiring changes in existing practices among the interagency.
- There is no whole-of-government DT threat picture, largely because the US Government does not have a common terminology to describe the threat. The absence of a common understanding of how threat departments/agencies prioritize DT issues differently results in a lack of analytic research and production on DT threats, and in turn reinforces the lack of policymaker prioritization.

Conference Panel Presentations and Working Groups

For each theme, a panel of experts provided introductory remarks and then facilitated working group discussions with conference attendees. The below summarizes the content of panel presentations and working group discussions and is not intended to represent the views of any particular department, agency, panelist, or participant.

Terminology

The terminology panel was led by experts from academia and FBI who discussed the implications of distinguishing between DT, homegrown violent extremism, hate crimes, and targeted violence. Key takeaways included:

- The US Government lacks a common definition and set of terms to describe DT; the current definitions derive from analysis of the criminal and violent actions of DT actors and are useful for departments and agencies with DT investigative missions, but are not easily adapted to those with intelligence or prevention missions;
- Terminology needs to be appropriate for applicable agencies at the federal, state, and local levels, create a common understanding of the threat, and must accurately depict an ideology or ideologies linked with criminal activity or violence;
- The US Government needs to find a way to increase public trust by being transparent with the public about how DT definitions are derived, defined, and used;
- DT and hate crimes are not mutually exclusive.

Terminology Working Group:

Obstacles & Solutions
Obstacles: • Interagency, IC, and local authorities lack awareness of how they each use terms differently based on their distinct mission roles. • Departments/agencies differ on their understanding, descriptions, and prioritization of the DT threat, which may inhibit analytic research and production. With limited or fewer analytic products, policymakers may conclude that DT is not a priority issue. **Solution:** • Convene the IC, state, and local law enforcement, academic, NGO, community service organizations, and foreign-partner communities to generate a comprehensive list of relevant DT terms and an explanation of how those terms are used.   ◦ Generate consolidated, consistent talking points for use with both policymakers and the public to better explain the DT threat and secure the resources required to address it. • Apply relevant lessons learned from international terrorism; provide policymakers with more IC products that put DT threats within the Homeland in the global political context.
What would derail US Government efforts against domestic terrorists?
• We can require all agencies to use the same terms and definitions despite each agency's need for different terms to fulfill their unique missions.

- We can undermine the public trust by failing to be transparent or clear about terms—how the US Government uses terms, what we mean by them, and how that may differ from the public's intuitive understanding of DT.
- We can face data challenges resulting from using terms that do not accurately/adequately capture the threat.
- We can fail to effectively explain to the public that the DT-IT distinction is largely a legal/authorities/bureaucratic one.

Authorities

The authorities panel included academic and civil liberties experts who discussed whether current DT authorities should be expanded, how, and against whom; the merits of applying terrorism designations in the domestic realm; and lessons that can be drawn from historical and foreign-partner case studies. Key takeaways included:

- Federal statutes designate many terrorism-related activities as criminal, but membership in groups with violent or extremist ideologies is protected until espousing violence crosses a threshold of intending to incite—or actually inciting—such violence;
- From a law enforcement perspective, a criminal DT statute could provide additional authority to open investigations, bolster information sharing, and may aid in securing DT resources;
- From the civil rights community's perspective, existing authorities sufficiently address DT; DT is a policy problem that requires better alignment of resources to the threat, not a law problem; most NGO representatives that attended the conference did not support designation.

Authorities Working Group:

Obstacles & Solutions
Obstacles: • Difficulty of differentiating extremist speech from mobilization-to-violence indicators. • Lone actors know how to operate without triggering law enforcement actions. • Ingesting and sharing US person(s) data constrained; government access to private sector data (Facebook, Twitter, etc.) is bound by collection authorities. **Solutions:** • Explore creating a DT criminal statute and/or designating DT organizations for deterrence purposes and provide additional federal violation to authorize predication of an investigation. • Legislation/litigation that defines research of publicly available information in the DT space; revise how to share Title III[1] information within the IC.
What would derail US Government efforts against domestic terrorists?

[1]Title III proscribes the interception of oral and wire communications collected under law enforcement authorities, "while making provision for law enforcement to intercept these communications for use in criminal investigations." 18 U.S.C. § 2510

- We can fail to fully understand the breadth of our own authorities or choose to narrowly interpret them out of risk aversion.
- Our criteria for publicly labeling attacks as DT is opaque and inconsistent.
- We can continue to charge DT actions as criminal rather than terrorism.

Operations

Experts from FBI and DHS discussed how different federal agencies approach DT and how we might shape future approaches. Key takeaways included:

- DHS is working to create a better understanding of the social ecology that drives radicalization and mobilization to violence to determine how and with whom to partner in the existing prevention arena;
- The US Government needs to improve on publicly communicating success and better involve communities in prevention efforts;
- Speech activities protected under the First Amendment of the Constitution should be viewed as a factor, not a constraint;
- Panelists noted that federal law enforcement's goal is to prosecute actors, rather than groups, that commit violations of federal criminal law. While a very narrow situation may permit state or local prosecution of DT cases in the absence of a federal criminal violation, all DT cases regardless of jurisdiction begin with a suspected violation of criminal law.

Operations Working Group:

Obstacles & Solutions
Obstacles: • Department/agency efforts to enable early identification of all types of terrorism, build effective community partnerships, and broaden information sharing are rarely integrated. **Solutions:** • Create a cohesive and coordinated US Government effort to publish, engage, and communicate among ourselves, with the private sector, and to the public.
What could derail US Government efforts against domestic terrorists?
• We can fail to resource DT efforts in proportion to the evolving threat. • We can fail to build an infrastructure for collection and sharing of DT information vertically among law enforcement and laterally with the private sector, civil society, and NGOs.

Expanding Partnerships

Experts from academia and industry led the final panel on expanding partnerships and addressed ways to enhance whole-of-government and public efforts to counter DT. Key takeaways included:

- Analysis of open-source information can help us identify DT trends. We need to build public-private partnerships in that space. Counties with the greatest amount of internet searches related to white supremacy are not located in states, indicating that DT is a localized, county problem that differs vastly across and within states;
- Tech companies are emerging as the dominant funder of research on violent extremism;

- US Government agencies with the responsibilities and authorities to do so should focus on expanding existing countering-violent-extremism tools to address DT rather than developing separate programs;
- The US Government should work with European allies to identify and apply lessons learned and best practices in countering DT;
- We need to determine what information private companies have that could enhance broader prevention efforts or specific investigations, examine the barriers to obtaining the information, and build trust with these companies to establish processes to do so; people share info on tech platforms that they do not share with school, friends, or family.

Expanding Partnerships Working Sessions Output:

Obstacles & Solutions
Obstacles: • When the US Government and its partners do not understand their distinct goals, they may work at cross-purposes and degrade support. • The US Government is a small player in the information environment, relying heavily on civil society and the private sector. • Law enforcement organizations, private sector, and civil society organizations, have different threat perceptions and absorptive capacities. • Institutional impediments to information sharing are broader than DT. **Solutions:** • Establish a clearer picture of what the US Government does and needs that is easier for civil society, NGO, and private sector partners to understand. • Apply lessons learned from state, local, and foreign-partner experiences in countering recruitment and radicalization.
What could derail US Government efforts against domestic terrorists?
• We can fail to provide sufficient support to civil society and state, local, tribal, and territorial partners as the primary actors in the DT space.

A Way Forward: Senior-level and US Government Experts

To conclude the conference, senior-level executives and experts from across the US Government met separately to begin shaping a way forward in the DT arena. Both groups recognized the need for a common DT terminology, as well as a common understanding of the DT threat throughout the Federal Government. To that end, both groups agreed to continue these conversations to address the evolving DT threat. In addition to NCTC's forthcoming DT assessment, NCTC will host working groups to continue these discussions and develop an interagency action plan for the DT mission space.