Adopting a Whole-of-Society Approach to Terrorism and Counterterrorism

Nicholas Rasmussen

Nicholas Rasmussen (@NicholasRasmu15) is the Executive Director of the Global Internet Forum to Counter Terrorism. He served as director of the National Counterterrorism Center (NCTC) from December 2014 until December 2017. He is a Non-Resident Senior Fellow at the Reiss Center on Law and Security at NYU School of Law.

On the 20th anniversary of 9/11, there is a genuine responsibility to assess anew the terrorism and extremism environment within which we in the United States currently find ourselves. Beyond that, we need also to consider with an open mind whether the strategy and policy approaches we have been relying on in the past two decades are well-suited to the evolving challenges we face.

As we approach that 20-year anniversary, my answer to the latter question is a clear "no." Particularly with the growing threat to public safety and security posed by domestic violent extremism, it is essential that we move beyond the post-9/11 counterterrorism strategy paradigm that placed government at the center of most counterterrorism work. Viewed from the perspective of a private citizen and former senior government official responsible for counterterrorism matters, there is a clear imperative to mature and evolve our counterterrorism strategies from a focus on integrating a "whole-of-government" effort to a much wider, more expansive and inclusive "whole-of-society" approach to addressing our terrorism and violent extremism challenges.

That wider circle must not only include state and local governments, but also the private sector (to include technology companies), civil society in the form of both individual voices and non-governmental organizations (NGOs), and academia. A whole-of-society approach promises to be in many ways more messy, more complicated, and more frustrating in terms of delivering outcomes. All that said, adopting this broader perspective offers the best chance of managing or mitigating the diverse, constantly changing threat we face from terrorism, particularly inside the United States.

Evolution of the Threat

In recent years, the most efficient way to track the federal government's evolving view of the terrorist threat to Americans has been to review the Annual Threat Assessment of the United States Intelligence Community. Publication of that document, and the ensuing public testimony before U.S. congressional committees by senior intelligence officials, represents the best chance for our Intelligence Community (IC) to speak publicly about its assessment of the full range of threats to U.S. national security. As in prior years, this year's assessment catalogues and updates the threat picture tied to Sunni terrorist groups like ISIS, al-Qaeda, and their various affiliates and networks around the world. Two decades after 9/11, that is largely familiar stuff, and that aspect of the threat promises to be persistent over time given security challenges in key conflict zones around the world.

Where this year's assessment breaks new ground for the IC is with its focused treatment of what the Community calls Domestic Violent Extremists (DVEs). The IC this year assesses that DVEs "motivated by a range of ideologies not connected to or inspired by jihadi terrorist organizations like al-Qaeda and ISIS pose an elevated threat to the United States." The assessment further notes that this "diverse set of extremists reflects an increasingly complex threat landscape, including racially or ethnically motivated threats and antigovernment or antiauthority threats."

Beyond the abbreviated treatment of the domestic extremism threat in its annual comprehensive assessment, the Office of the Director of National Intelligence (ODNI) went on to publish a more focused threat assessment of the DVE problem in March of this year. The IC's effort to elevate analysis and discussion of the threat posed by DVEs is important because it puts the federal government on record and helps signal heightened priority focus across the CT and homeland security enterprise, which ultimately will help drive resource allocation.

But this year's assessment hardly comes as any surprise given the increased prevalence of domestic terrorist attacks or events we've seen in recent years. Indeed, if most Americans were asked if they felt more at risk from a homeland terrorist attack linked to a domestic group/actor or to an overseas group/actor, I suspect the large majority would cite the DVE threat as feeling more imminent and more acutely dangerous to the average person living in the United States. And statistically, it is, indeed, the greater threat. As the *Washington Post* has noted, nearly every state has catalogued at least one domestic extremist incident or plot in recent years, suggesting that there the reach and potential impact of the DVE problem has eclipsed other forms of terrorism here inside the United States.

The net result of this evolving threat landscape is that domestic terror concerns now sit alongside homeland threats linked to overseas terrorist groups or ideologies, on roughly equal footing in terms of the level of urgency, political salience, and policy prioritization. Perhaps the best evidence that this transformation of the threat picture had taken place was the early effort by the incoming Biden administration to prioritize the development of fresh approaches to address domestic extremism and terrorism. This was almost certainly intended to be an early priority for President Biden's team even before the events of Jan. 6 at the U.S. Capitol, but the attack on the Capitol certainly added impetus to the effort.

The announcement on Jan. 22, 2021 of a domestic terrorism policy review led by the National Security Council (NSC) staff and the fast-track development of a National Strategy for Countering Domestic Terrorism signaled early urgency and immediate focus at the highest levels of the Biden team. These moves also suggested that the new administration did not feel adequately postured to address this particular threat landscape in terms of the strategy, programs, and resource framework that it inherited from the Trump administration.

What Does the Changing Threat Landscape Mean for CT Strategy?

This evolution in the threat landscape should cause us to reexamine with a critical eye the set of tools, strategies, and structures that we are using to respond. For the entire post-9/11 period, senior officials under the Bush, Obama, and Biden administrations have touted their development of "whole-of-government" approaches to addressing the CT challenges we faced, mostly from abroad. In so doing, we aimed to reassure the American people that the federal government was taking an expansive, creative approach to keeping them safe. We were not simply relying on one set of tools tied to our law enforcement community or another set of tools operated by either our military or our intelligence community. That whole-of-government mindset was also driven by the painful self-examination and lessons learned exercise that followed the 9/11 attacks. The 9/11 Commission recommendations certainly pointed to a need for a more coherent and coordinated federal response to terrorism, but even without that roadmap, counterterrorism professionals knew instinctively that new ways of doing business across government were required to respond to the al-Qaeda threat.

A whole-of-government approach meant that whenever we confronted a particular terrorism problem, the White House and NSC staff would organize an effort to bring all tools and instruments of national power into an integrated effort to address that problem. These diverse tools, to be orchestrated and sequenced, included the use of military power when absolutely necessary, but also diplomatic influence, intelligence operations and collection and analysis, law enforcement operations, capacity building, financial tools, international development and foreign assistance programs, and our strategic communications capacity.

Embedded within the whole-of-government approach to terrorism was a presumption that the federal government was not only the primary actor when it comes to terrorism and counterterrorism work but in most cases the *only* actor of consequence in terms of being able to deliver positive outcomes and mitigate threats to Americans. We of course were also heavily reliant on the capacity of state and local governments and partners responsible for their share of the homeland security enterprise. But for the most part, development and execution of counterterrorism strategy was a Washington-centric project for both Republican and Democratic administrations since 9/11. Today's evolving threat landscape, and in particular the emergence of a dramatically heightened threat from domestic violent extremists, renders that whole-of-government approach to counterterrorism wholly insufficient.

Toward a Whole-of-Society Approach to Countering Terrorism and Violent Extremism

While we should not absolve government of its obligation to lead and organize societal response to the problem of terrorism and violent extremism, the set of actors and sectors with at least some degree of responsibility for contributing to solutions extends well beyond government. We stand a much better chance of achieving results with our CT strategies if those strategies reflect input and active participation from that diverse set of stakeholders beyond government and seek to harness the knowledge, expertise, and comparative advantage that exist outside the classified circle of CT experts centered in Washington. This wider set of contributors, or stakeholders, includes:

The private sector, including technology companies. In the past, content associated with known Salafi-Jihadi terrorist groups like al-Qaeda and ISIS was widely available on larger, more mainstream social media platforms. It is also true that many of those platforms have invested significant effort and resources in building content moderation capabilities to remove that content when it violates

their terms of service frameworks. Today, terrorists and violent extremists continue to take advantage of the online environment to further their agenda, but the problem has expanded to include exploitation of many different online service providers and different components of the technology stack by a broader range of actors and organizations across the ideological spectrum. That evolving reality imposes on the private sector special responsibility to be more creative and agile in the effort to develop effective tools, policies, and approaches to addressing terrorist or violent extremist content or activity on their platforms and services. Clearly, more needs to be done by industry to limit the ability of terrorists to exploit the online environment.

At the same time, the many questions private companies face in this context are not easy and many potential solutions come with unintended consequences. Countering terrorism and violent extremism are important societal objectives, but those objectives cannot be pursued at the expense of other equally important principles and priorities, to include respect for fundamental human rights such as freedom of expression. When companies look to governments for guidance in the form of law or policy with respect to many of these complicated questions, what they often see is an incomplete and sometimes conflicting patchwork of measures and legal frameworks.

When we take stock of the last several years of back-and-forth between the U.S. government and the technology sector on this set of problems, it's possible for two things to be simultaneously true. Several of the largest and most prominent tech companies have shown a willingness to tackle these problems more aggressively, to devote significant resources to that work, and to deepen their conversation with government about those efforts. At the same time, clearly, much more work needs to be done by those leading companies and by governments to eliminate terrorist activity on the internet as the problem of online terrorism and extremism continues to evolve.

Put simply, government and the private sector, certainly for the foreseeable future, will each have a critical role to play in addressing the societal challenge of terrorism and violent extremism. Governments look to companies to be more effective and forward leaning in promptly enforcing their terms of service. Companies increasingly look to governments for greater clarity on the policy and legal landscape, reducing the need for companies to go it alone in making decisions about designation frameworks or banned content. Creating open channels for that dialogue is essential. The organization of which I am the Executive Director, the Global Internet Forum to Counter Terrorism, or GIFCT, serves as one of those vehicles for collaboration and dialogue between and among the various actors.

Civil society, to include the full array of relevant NGOs and independent voices. The ways in which civil society voices and organizations can contribute to CT strategies, particularly in the context of DVEs, is worthy of a much longer discussion than this essay allows. Suffice to say that much of the most important and effective work being done to prevent the spread of hatred, violent extremism, and targeted violence takes place at the local or community level. It is encouraging that the Biden administration has moved quickly to capitalize on that source of strength by both emphasizing this work as part of its new national strategy, while also planning to expand the pool of federal funds available to support it.

Civil society voices also play a critical role in engaging with government and the technology sector on terrorism questions, particularly with respect to content moderation, to ensure that the work undertaken in pursuit of CT objectives has the impact of advancing fundamental human rights, especially freedom of expression. Inclusion of civil society voices in the effort to develop effective CT strategies increases significantly the chances that those strategies will be reflective of society as a whole and broadly consistent with our set of collective values.

Academics and other subject matter experts. One of my most embarrassing personal blind spots during my period of government service working on terrorism issues centered on my failure to appreciate just how much knowledge and expertise existed outside of government on the problem that I was focused on inside government. Those of us "inside" tended to believe, or at least to act like, we had access to the best information and that our strategic insights were therefore informed by that knowledge advantage. Sitting outside government as I now do, that mindset seems myopic at best and absurdly self-defeating at worst. The deep reservoir of expertise and information on all forms of terrorism and violent extremism that exists outside of government remains untapped in my view. That is partly a result of the focus and investment of resources in the academic world that has taken place over the last twenty years. It is also a reflection of the fact that so much terrorism information and activity resides or is accessible in the open source environment, where a government analyst is no more privileged with access than any other smart terrorism expert.

The glimmer of good news is that the Biden administration's new Domestic Terrorism strategy plainly acknowledges that government does not have a monopoly on wisdom or information with respect to this problem. The strategy calls upon DHS to "create a structured mechanism for receiving and sharing within government credible non-governmental analysis." That's an important admission that successful government strategies will hinge on input, analysis, and information from outside government, where relevant expertise is available.

Other governments. Collaboration between the federal government with both state and local governments here in the United States and with partner governments abroad has long been a feature of U.S. CT strategies. That collaboration needs to deepen even further as CT resources are redirected to address other high priority national security challenges. Terrorists, even domestic terrorists, will continue to show a complete disregard for international borders. Terrorist and extremist narratives circulate freely across the world, as does relevant expertise, advice, and encouragement. That content is also translated and localized for particular audiences all over the world. Any successful approach to our CT problems will contain an important degree of both burden sharing and tangible cooperation with governments at every level.

Having argued that successful CT strategies must be more inclusive and reflective of the genuinely multi-stakeholder nature of the problem, I would not make the case that involving the full array of stakeholders is easy or always comfortable. More voices representing more constituencies can often bring more discord, disparate and competing priorities, and multiple paths to solutions that are often at odds with each other. A whole-of-society approach to our CT problems is certain to be messy, complicated, and at times very unrewarding. It may not be possible to devise policies or strategies that are acceptable to all of the various participants. The effort to arrive at a common set of solutions to a complex problem like terrorism, especially given the diverse nature of the stakeholder community, may seem literally impossible. And yet, working outside that multi-stakeholder framework ultimately limits the efficacy and impact of CT strategies before they are even conceived or developed.

Innovation of Institutions

If it is true that whole-of-society, multi-stakeholder engagement is essential to the effort to develop and implement sound CT strategy and policy, then where and how should that engagement take place? What institutions and fora can we potentially look to for inspiration and example as we try to create and mature this sort of innovative framework for policy development? Unfortunately, there is not a great deal of history on which to draw in this space and I would argue that this work is still very much in an early proof-of-concept phase. That said, there are in fact nascent efforts to create just these sorts of engagement frameworks.

One of those, the Christchurch Call, emerged out of the horrific attack on members of the New Zealand Muslim community in March 2019. Organized and driven by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron, the Christchurch Call has brought together in common cause more than 50 countries and

governments with almost a dozen of the major online service providers. That assembly of Call supporters is bolstered further by an Advisory Network that includes dozens of civil society organizations from around the world. In only its second year of existence, the Christchurch Call forum has quickly become an essential convening ground for government, technology companies, academics, and civil society as they work together to eliminate terrorist activity and content online.

The organization of which I am the Executive Director, the Global Internet Forum to Counter Terrorism, or GIFCT, is similarly postured to carry forward this multi-stakeholder work to counter terrorism, and specifically its online dimensions. GIFCT was initially formed in 2017 by YouTube/Google, Facebook, Microsoft, and Twitter for the purpose of bringing together key technology companies to collaborate across traditionally competitive company lines to pursue the shared objective of preventing terrorists and violent extremists from exploiting the internet. GIFCT also maintains a robust connection to civil society and government through its own International Advisory Committee (IAC), its multi-sector thematic Working Groups that convene to address hard problems at the nexus of technology and terrorism, and to the academic world through its research and scholarship arm, the Global Network on Extremism and Technology.

Both of these organizations are still early in their development and are testing the limits of what is ultimately possible. Over the last year, I have experienced firsthand how worthwhile this trial effort to utilize multi-stakeholder approaches to public policy challenges can be. What these fora have already proven is that they can be essential convening bodies for discussions about the nature of the evolving terrorist threat, the set of common objectives that should be pursued to mitigate that threat environment, and about measures of success in the overall effort to counter terrorism online.

Reaching consensus around big questions such as these is no small feat and represents an important step forward in efforts to craft whole-of-society approaches to one of our most pressing national security challenges. Participation in these multi-sector processes and fora also helps create accountability as each participant is expected to speak clearly to the work they are doing and the results that their work is producing. Driving real progress and delivering concrete CT results that mitigate and reduce the threat from terrorism, while striving to be inclusive of critical diverse voices and committing to be more transparent in our processes, is the next challenge on the horizon.