Send Airplanes, Phones, and Money: Cautionary Lessons For the Post-1/6 World from the Post-9/11 World

Paul Rosenzweig*

INTRODUCTION 179
I. CONFRONTING THE 9/11 TERROR NETWORKS 180
II. CONFRONTING DOMESTIC TERRORISM TODAY 182
CONCLUSION 185

INTRODUCTION

Twenty years ago, September 11, 2001 dawned clear and bright: a perfect fall day in the District. I was a young-ish lawyer and spent the morning in a conference room—oddly enough with, among other people, John Roberts, who was then an attorney in private practice—cut off from the events occurring outside. Nobody came into the room to tell us that the world had changed, and yet it had.

When we emerged around noon into the light of day, legal specialties that until that time were backwaters or afterthoughts of policy and law had become in an instant the focus of intense concentration and scrutiny. For myself, I went from being a criminal lawyer with limited experience in terrorism surveillance law to embarking on a career path that led me to spend most of the past twenty years thinking about homeland security and counterterrorism issues, along with their related, near-cognates such as cyber and aviation security.

From the vantage point of twenty years onward, the confusion and palpable concern—dare one say "fear"—coursing through our body politic at that time is difficult to remember, yet it strangely seems all too familiar today as our nation faces a different sort of crisis. Our task in this series of commemorative essays is to look at what worked and what didn't work in the counterterrorism regime over the past twenty years and to determine what that means for today and tomorrow. For my part, that translates to the question, what—if anything—should the Biden Administration's leaders of homeland security take away from our experience of the past two decades?

From a standing start, we learned much about how to combat foreign terrorism that targeted its effects on American soil. Those lessons were hard won, yet of real value. The challenge for the next twenty years will be translating those

* Professorial Lecturer in Law, George Washington University School of Law; former Deputy Assistant Secretary for Policy, Department of Homeland Security (2005-09). The title of this article is an homage to Warren Zevon, whose song "Lawyers, Guns, and Money" captures some of the urgency in the policy world in the immediate aftermath of September 11th and today. WARREN ZEVON, *Lawyers, Guns, and Money*, *on* EXCITABLE BOY (Asylum 1977). © 2021, Paul Rosenzweig.

lessons in the face of a mutating terrorism threat. Today, the threat is domestic rather than foreign, and the lessons of 9/11 are much more difficult, if not impossible, to apply to the mutating post-January 6 threat stream.

I. CONFRONTING THE 9/11 TERROR NETWORKS

September 11th was a strategic surprise, both in the methodology used to attack the Nation and in the idea that our home soil was vulnerable. We were confronted, almost immediately, with the idea that most of our strategic theories of defense—for example, that the homeland was safe behind giant ocean barriers—were of limited utility. We were likewise confronted by the fact that our perception of our strategic enemies was equally deficient: our biggest threats were no longer other nation-states like Russia and China, as smaller, more nimble foes had killed Americans on American soil, and we had no plan for counteracting their efforts.

We had to develop one on the fly. The first Secretary of Homeland Security, Tom Ridge, has been quoted, perhaps apocryphally, as likening the process to building an airplane in flight. The Department of Homeland Security was created without any structural scaffolding and without any policy for how to fight the fight it was tasked with winning.

However, within a year or so, the outlines of a strategy began to emerge. The tenets were never formally codified (at least not in any public document I ever saw), but if I could characterize the counterterrorism strategy we developed, it would be something like this:

- *Disrupt the terrorist activity*. Everything the enemy does requires organization; disrupt it as much as is feasible.
- *Extend our border*. Move screening offshore as much as possible. A threat interdicted abroad is a threat that doesn't reach the homeland.
- *Defend in depth*. Each defensive system has its weaknesses; if the systems are independent of each other and you layer them appropriately, you amplify the defense and diminish the risk.[1]

The broad outlines of this strategic approach eventually became operationalized in Departmental activity. For example, as part of the idea of defending in depth, DHS layered Secure Flight digital screening (that is, the current system where travelers provide their name, date of birth, and gender for pre-flight identification and screening) on top of TSA's physical screening, backed by hardened cockpit doors and armed Federal Air Marshals. Again, though we didn't initially

1. These are the homeland defense pillars of the strategy as it was built. A fourth pillar—and perhaps the one that was most effective—was the military one of engaging the enemy at his base. Whether the war in Afghanistan was worth it or not is a question I cannot answer, but I think we can say with a high degree of confidence that our engagement there was "covering fire" that forced our enemies to engage abroad, diverting their resource and attention from further attacks on the homeland.

articulate the theory formally, we understood that multiple independent layers of defense were more likely to be effective than a system with a single point of failure.

The concepts of organizational disruption and the extension of our borders led to an operational plan that became the heart of DHS preventative counterterrorism activity. As my title "Airplanes, Phones, and Money" suggests, we focused our tracking and disruption efforts on three of our adversaries' operational activities that seemed to be necessary for any successful terrorist attack: travel, communications, and funding. While it is too strong an argument to assert that these preventative actions were *the* cause of our success in preventing a second 9/11, I would ascribe to them significant preventative value.

The first part of our theory was that the terrorist would have to travel to America from overseas (this was before the advent of the next phase of the foreign terrorist assault when radicalization in place became more frequent). To disrupt this travel and conduct screening overseas, we developed a number of systems for the analysis of terrorist threat data relating to those who would travel to the U.S. One such system was the mandate that airlines provide DHS with the passenger name records (PNRs) for all travelers bound for our shores. DHS would then screen that PNR data against the lists of known or suspected terrorists and other intelligence sources to identify individuals whose travel posed greater risks. Though most of the screening program's successes remain classified, it was apparent to me that the number of true positives identified by the program was quite substantial and of significance.

Second, we understood that any terrorist activity would require coordination and communications. To this day, the NSA's collection program, operated under Section 702 of the Foreign Intelligence Surveillance Act, remains controversial, to say the least.[2] However, it too was a critical tool in disrupting terrorist activity and a source of intelligence about planned attacks that assisted in our efforts to deter terror. Indeed, in the late 2000s and early 2010s, Section 702 data is said to have made up as much as 25% of the President's daily intelligence threat briefing.[3] We know as well that foreign adversaries had to modify their communications structures to avoid detection, a sign that, at least to some degree, the interdiction of their communications was having the desired effect.

Third, we thought that terrorist activity would require significant funding, so the U.S. initiated a money tracking program that involved the review of international money transfer activity. These reports were created by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgium-based organization. Like PNR and Section 702, the creation and analysis of these reports was not without controversy, so much so that the reviews are now severely circumscribed because of international privacy concerns. Nevertheless,

2. Foreign Intelligence Surveillance Act § 702, 50 U.S.C. § 1881a.

3. *See generally,* PRIV. AND CIV. LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 108 (2014), https://perma.cc/ZB46-ERGY.

the SWIFT reviews were of great utility in identifying potential terrorist risks and tracking terrorist finances across the globe.

By and large, this system worked. I certainly would not ascribe all of our success in defending the homeland against foreign terrorism to this operational concept—and as noted earlier, it is likely that the war in Afghanistan played a significant role in our efforts—but it is nonetheless apparent to me that these concepts had some degree of success in disrupting attacks.

Indeed, the best indication of our success was that our adversaries had to adapt and change tactics. The so-called "second wave" of terrorism involved domestic actors who were radicalized in place through propaganda, a change that limited the need for international travel, reduced funding requirements, and involved communications through overt social media channels instead of covert methods. We are still struggling today to identify a successful counterstrategy to combat this mutated threat.

II. CONFRONTING DOMESTIC TERRORISM TODAY

If September 11 was a strategic surprise, the threats to America in the post-January 6 world are even more astonishing in the way they disrupt settled expectations. Prior to this past year, few if any would have seen America's commitment to democracy, openness, and freedom of expression as strategic weakness; we would have touted it as our great strategic advantage, the very hallmark of American exceptionalism. Yet in the aftermath of January 6, those same advantages are barriers to an effective response, and we have yet to come to grips with that reality.

Consider how the lessons of 9/11 are applicable and—more saliently—inapplicable today. The nearest analog we have is the second wave of radicalized terrorists in place, a challenge we have yet to adequately respond to. However, the challenges of this second wave of foreign terrorism are less than those from domestic terrorism, as the legal and policy problems are compounded further when we talk about responding to internal threats of violence.

The challenge from domestic terrorism is real. As President Biden has said: "Make no mistake – the terrorist threat has evolved beyond Afghanistan since 2001 and we will remain vigilant against threats to the United States, wherever they come from. . . . [W]e won't ignore what our own intelligence agencies have determined – the most lethal terrorist threat to the homeland today is from white supremacist terrorism."

Though some doubtless disagree, viewing this assessment as politicized, the limited data available seems to indicate that far-right domestic extremism is increasing at a much faster rate than other forms of domestic violent action.[4] And so, many observers would look at the events of January 6 and agree with DHS

4. WILLIAM S. PARKIN, JEFF GRUENEWALD, BRENT KLEIN, JOSHUA D. FREILICH, AND STEVEN CHERMAK, ISLAMIST AND FAR-RIGHT HOMICIDES IN THE UNITED STATES (Infographic) (National Consortium for the Study of Terrorism and Responses to Terrorism 2017), https://perma.cc/8XCD-VTSH.

Secretary Alejandro Mayorkas: "Domestic violent extremism poses the most lethal and persistent terrorism-related threat to our country today."

However, how we respond to this threat remains uncertain. As mentioned previously, in many ways the new domestic threats pose the same sorts of challenges as the second wave of foreign threats. Like the second wave, the new threats do not arise overseas, and they metastasize at least partly on public communications channels rather than covert ones.

That being said, the domestic threat poses even greater policy challenges than we see in confronting foreign terrorism. Many factors will make systematically responding to domestic terrorist threats (like the one posed by the January 6 attack on the Capitol) exceedingly difficult. Indeed, the sad truth is that lessons we have learned from fighting foreign terrorism demonstrate that using the same tools to fight domestic terrorism is nearly impossible.[5]

Given the constitutional freedom to travel, travel limitations are more problematic in the domestic context, as the domestic equivalent of a foreign PNR exclusion is less plausible and legally more fraught. The legal threshold for being added to the terrorist watch list is properly higher for American citizens than it is for foreigners, and there is an understandable reluctance to identify as a terror threat our fellow citizens who, in a different light, are merely exercising the right to political dissent.[6] That reluctance is, in turn, tied to understandable fears of the misuse of federal authority. Thus, we are unlikely to see the adoption of a PNR-like screening system or additions to the domestic no-fly list that are based solely on participation in questionable events or domestic political activities, even where those activities may be pregnant with the threat of violence.

Instead, we can conceive a system of scrutiny tied to known actions and actual violence. For example, reports exist of airlines denying boarding to those who have been charged with participation in the events of January 6. However, it seems highly unlikely that the government will systematically make available a list of those with known or suspected ties to, for example, the Proud Boys. It is

5. In the text that follows I discuss the airplane/money/phone trilogy of pathways to disruption, but there are many other intractable hurdles in the domestic context. For example, the constitutional right to keep and bear arms brings with it the reality that the easiest solution—limiting access to weaponry—is utterly untenable in the near to mid-term.

6. While we have a working definition of what we mean by domestic terror (the FBI defines it as "violent, criminal acts committed by individuals and/or groups in order to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature," Fed. Bureau of Investigation, *What We Investigate: Terrorism*, FBI.GOV, https://perma.cc/UF6J-LXGL, and the PATRIOT Act has an even more detailed definition, *see* 18 U.S. Code § 2331(5) (defining the activities of domestic terrorism)), we have no legal structure for designating groups that engage in domestic terrorist activities. The Secretary of State has long been able to formally designate Foreign Terrorist Organizations (FTOs), but no parallel authority to designate DTOs exist in law (though President Trump did make a fitful attempt to designate "Antifa" as a DTO). *See* Reuters Staff, *Amid Protests, Trump Says He Will Designate ANTIFA as a Terrorist Organization*, REUTERS (May 31, 2020, 1:09 PM), https://perma.cc/J7UQ-LWTY. Given the political "third-rail" nature of designating domestic terror groups we should, as an initial matter, look for implementation cases that don't rely on such a designation.

even more unlikely that the government would ask airlines to deny those people boarding or flag them for scrutiny when they make a reservation. Therefore, we face the prospect that travel interdiction will be of limited use in confronting domestic violence.

Likewise, a focus on financial surveillance is likely to be of little value. For one thing, funding needs for domestic terror are less substantial than for foreign-originated terror, because the costs of conducting the attack are relatively less, and some of the activity may be funded by like-minded domestic supporters whose financial support will be difficult to track. Funding transfers will often be difficult to observe given domestic banking laws that, quite rightly, highly value individual privacy. Early in any investigation, without discrete groups and bank accounts to target, domestic terrorist financing scrutiny is likely to be ineffective at identifying financial flows or individuals' activity. The financial screening will be of use, if at all, only when the threat is more imminent; it will be an investigative tool rather than a disruptive one.

Finally, and most problematically, much of the communications related to domestic threats bump up incredibly close to protected First Amendment advocacy. We have seen the blurring of the lines already: violent domestic networks will frequently involve individuals who are radicalized and mobilized through social media that, for the most part, involves the protected expression of opinion. It is difficult, if not impossible, to imagine a world in which the government interdicts those communications given that even routinely monitoring them is so controversial.

Once mobilized, their organizational efforts will be backed by the use of encrypted communication platforms. While it may be that the threat of domestic violence finally leads to Congressional action mandating forms of extraordinary access to encrypted platforms, that seems highly speculative, to say the least, and it will be vigorously resisted. Even if we were to succeed in doing so, the effort may prove of little value. For domestic terror groups, even more than for foreign terror organizations, their communications are diffuse and leadership is difficult to identify, and indeed, in some cases it may not exist at all.

For these reasons, the active or passive monitoring of domestic communications is deeply disturbing; it runs directly against our basic sense of what makes the U.S. different from other nations. It raises the hackles of civil libertarians, with good justification, and off-loading the monitoring of these communications to social media platforms under the guise of content moderation brings with it its own set of challenges, as the recent Facebook Oversight Board relating to President Trump makes clear.[7]

However, it seems to me that this is the lesser of all evils in terms of policy. In practical terms the only reasonable option is for those seeking to prevent domestic terror to work at developing early warning systems within existing communications

7. *See* Case decision 2021-001-FB-FBR (May 5, 2021) (upholding Facebook's decision to suspend former President Trump's Facebook account), https://perma.cc/8R6D-TCJC.

networks and hope that we are able to react with sufficient alacrity—a characteristic lacking in our January 6 response—to potential threats as they arise. The key to countering domestic terrorism seemingly requires better and more nuanced intelligence collection within social media and within organizations that foster violence. As previously noted, however, this course is controversial, given the salience of First Amendment political concerns, but passive engagement is the least-intrusive method we can devise, and the alternative—to do nothing and allow the violent instincts to flourish—is an unacceptable choice.

The Department of Homeland Security already seems to be moving in this direction, having just announced a new social media early-warning system.[8] Properly scoped, it will operate at the strategic level—that is, not focused on individuals—and, one hopes, be deployed with sensitivity to civil liberties. Though there are risks even to this modest first step, but given what we think we understand about how domestic terrorism is enabled and energized, it seems the least-bad option.

CONCLUSION

None of our tactics learned after 9/11 fit well into the domestic counterterrorism model. For domestic terrorism, we need a new, different model. Instead of pushing our borders out and defending in depth, we need to think about how to deter terrorist activity through a combination of persuasion and sanctions.[9] Instead of trying to disrupt planning for domestic violence, we need to figure out how to persuade our domestic actors not to act in the first place, and how to appropriately monitor them when we cannot persuade them. It is a much more difficult and challenging issue set, precisely because it involves our fellow citizens.

Where we had relative freedom of action in confronting the foreign terror threat, constrained only by international law—which, while important, was of limited practical impact—in confronting domestic terror our responses are hedged around legal restrictions and historical practices, none of which we would want to jettison at the risk of damaging our democracy. Instead of airplanes, phones, and money, we need a different approach. Frankly, if I had an easy answer to what that approach should be, this would be a different essay. But perhaps the first step in solving a problem is recognizing that it is different from ones you've encountered before.

---

8. Ken Dilanian, *DHS Launches Warning System to Find Domestic Terrorism Threats on Public Social Media*, NBC NEWS (May 10, 2021, 4:30 AM), https://perma.cc/6YRG-NPQK (outlining a DHS program to gather and analyze intelligence from domestic social media posts akin in spirit, if not in legal basis or scope, to the type of post-9/11 collection directed abroad).

9. In this brief note, I have left aside other aspects of our strategy that might have analogs in the domestic context, such as defending in depth. If I may be permitted a personal reflection, however, I find the institution of permanent physical security features deeply problematic. The recently removed fencing around the Capitol was not defense in depth, but rather an open wound in our democracy. If we can do no better than to cower behind our walls, our government is not worthy of respect.

***