Critical Infrastructure & the Emerging Market for Domestic Terrorism

Maggie O'Connell[1]

Abstract:

This paper examines the modern threat landscape to critical infrastructure in the context of the existing legal framework for domestic terrorism. The United States has developed a conceptual understanding of terrorism perpetrated by foreign individuals and groups, but homegrown actors, many of whom have no clear ties to violent jihad, are increasingly prevalent, sophisticated, and misunderstood. Domestic terrorists are capitalizing on emerging, lesser known attack vectors, including insider access, cybersecurity breaches, and drones. This burgeoning market for terrorism requires a more holistic legal and regulatory approach to ensure our nation's critical infrastructure asset owners and operators are empowered to defend against these threats, and that federal investigative and prosecutorial bodies can effectively respond.

Keywords: Domestic terrorism, critical infrastructure

CRITICAL INFRASTRUCTURE ASSET OWNERS and operators are no strangers to the threat landscape in which their facilities reside.[2] Companies invest millions of dollars annually to secure their fencelines, patch their cybersecurity vulnerabilities, and develop protocols and procedures to comply with regulations seeking to mitigate and prevent terrorist activity. The safety and security of facility operations, personnel, and the surrounding communities are the goals of these investments, and critical infrastructure companies cannot afford to shortchange in any of these areas. Nevertheless, the threat landscape often evolves so quickly that the legislative and regulatory frameworks fall vastly behind the curve. The nation becomes the victim of a divisive political climate, a lack of understanding, and a general distrust for big corporations. What remains is a door wide open to nefarious actors and emerging threats, the vast majority of which are not yet completely understood nor accounted for in the law.

Although guns, guards, and gates are still the first lines of defense along a fenceline, they can provide a false sense of security. In February 2016, two airport employees in Somalia facilitated the transfer of a sophisticated bomb built into a laptop through airport security, where it was carried onto plane and detonated (Kriel and Cruickshank, 2016). Malware stormed the Ukrainian industrial control systems (ICSs) in 2015, 2016, and again in 2017, the latter effectively shutting down the government and key critical functions, including the radiation monitoring system at the Chernobyl nuclear power plant (Greenberg, 2018). In September 2019, a series of drone attacks at Saudi Aramco oil processing facilities in Abqaiq and Khurais in eastern Saudi

[1] Regulatory Affairs Specialist, American Fuel & Petrochemical Manufacturers Association, moconnell@afpm.org 1800 M Street NW, Suite 900 North, Washington, D.C. 20036

[2] The Department of Homeland Security (DHS) Cyber and Infrastructure Security Agency (CISA) outlines "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS 2019a).

Arabia forced the country to shut down half of its oil production capacity, to the tune of 5.7 million barrels per day (Li, 2019). This attack was a major blow to both the country and the global markets. Meanwhile, extremist environmental justice activists are turning pipeline valves, potentially causing harmful spills, injuries, and catastrophic explosions that could cripple the very communities they seek to protect (Williams, 2016).

Although some of these examples did not occur in the United States by homegrown actors, they all could have, and these are real cases of activities that skirt existing U.S. laws and regulations intended to safeguard critical infrastructure from domestic terrorist activity. Currently, U.S. critical infrastructure owners and operators have little-to-no recourse when it comes to such threats. The nation must understand that homegrown violent extremists (HVEs) are capable of carrying out attacks previously perpetrated by foreign-born terrorists. A reactive approach to terrorism does little to thwart the threat, and near misses can very quickly turn into hits without the proper statutes in place to give relevant authorities the license to enhance their pre-attack intelligence gathering and investigative efforts. There must be accountability in the legal and regulatory framework to investigate and prosecute those persons who tamper with, attack, and threaten any critical infrastructure operation in the United States.

Understanding Domestic Terrorism

The concept of domestic terrorism in the United States is complex. Domestic terrorist activities are often understood as mass shootings at soft targets and crowded places, and certainly qualify as terrorism. However, this only represents one aspect. As the lead agency for investigating terrorist activity, the Federal Bureau of Investigation (FBI) classifies domestic terrorism as U.S. persons who commit criminal acts based on their "political, religious, social, racial, or environmental" ideologies, rather than for monetary purposes (FBI, 2019). This definition illuminates an important component of domestic terrorism that is often understated in the context of threat analysis: a criminal act does not need to result in mass casualties to be investigated as an act of terrorism. From a prosecutorial standpoint, the Department of Justice (DOJ) views domestic terrorism as activities that:

(A) involve acts *dangerous to human life* that are a violation of the criminal laws of the United States or *of any State*;
(B) appear to be intended –
  (i) to intimidate or coerce a *civilian population*;
  (ii) to influence the policy of *a government* by intimidation or coercion; *or*
  (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; *and*
(C) *occur primarily* within the territorial jurisdiction of the United States [emphasis added] (18 U.S. Code § 2331.5)

Given this broad definition, there is no single crime of "domestic terrorism." Gaps exist in the federal statute and are ripe for exploitation, particularly via emerging threats. Although a person or group involved in a targeted attack will not escape prosecution, the charge may not fall under the *federal* terrorism statute. State criminal laws offer some avenues for penalizing terrorist activity, but punishments vary greatly state-to-state.

Chapter 113B of Title 18 of the U.S. Code remains the federal statutory guide for terrorism, but the crimes described therein are somewhat limited to foreign terrorism in that many require a

transnational or foreign element in the fact pattern. Although a few can apply to domestic terrorist activity – most notably through an interstate commerce element – the language in these statutes do not effectively capture emerging threats. They cover the use of traditional explosives or assume that lone actors and small, very loosely coalesced groups cannot easily rise to the level of active terrorists. In today's threat landscape, such assumptions create an environment in which terrorists can use emerging technologies and techniques to maximize devastation with limited effort and at minimal cost.

Emerging Threats

Over the last several decades, domestic terrorists have targeted critical infrastructure to advance political or social justice agendas. However, some maintain that domestic terrorists lack the organizational capacity and technical wherewithal to accomplish any meaningful attack on critical infrastructure (Riedman, 2017). This argument is myopic. Although it is true that the number of successful attacks against critical infrastructure in the United States is historically small, it is not prudent to rest on our laurels with respect to the nation's critical functions.[3] A successful attack need not be from a formally organized group. In fact, the FBI notes that current threat actors are typically "autonomous and lone offenders, and small cells pose the greatest threat" (McGarrity and Brzozowski, 2019). Evolution and access to technologies, open markets, and the dark web make homegrown terrorists just as organized as the international groups traditionally associated with terrorist activity. Earlier this year, Assistant Director of the Counterterrorism Division at FBI, Michael McGarrity, noted domestic terrorism is "on the rise" (Levine, 2019). Indeed, three factors actively contribute to the growth and evolution of this threat landscape according to the FBI: the internet, use of social media, and HVEs.[4]

In 2018, the FBI investigated 50 reported incidents, threats, or suspicious activity at pipelines alone (McGarrity and Brzozowski, 2019). In that same year, the FBI investigated 87 reported threats to refineries (McGarrity and Brzozowski, 2019). These are real, credible threats. In fact, on September 19, 2019, a federal grand jury returned an indictment charging two women with knowingly and willfully damaging and attempting to damage the Dakota Access Pipeline, causing "a significant interruption and impairment of a function of an energy facility" (DOJ, 2019a). The women made no secret of their efforts to sabotage the pipeline to advance a political agenda, by burning exposed valve sites and attempting to pierce portions of empty pipeline with torches (Schiano, 2019). These acts are dangerous to human life, in violation of the laws of the country and state, and are intended to influence the policy of the government. However, there is no mention of domestic terrorism in the indictment because the federal terrorism statute does not account for these types of attacks. Prosecutors must instead rely on other criminal laws to charge offenders - most of which carry far more lenient sentences.

Although these women operated as part of a larger extremist environmental justice movement, lone or small cell insider threats are another increasingly significant concern in the security space. Apart from a disgruntled employee carrying out a devastating, mass casualty attack on facility property, insider threats can take the form of economic espionage, cyber hacks, and –

[3]"Critical functions" is a term used by DHS CISA, and is defined as: "The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS, 2019b).

[4] Currently, the FBI is investigating suspected HVEs in every state and view HVEs as a primary terrorism threat in the U.S. The FBI defines an HVE, in part, as someone who "receive[s] no individualized direction from terrorist groups" (FBI, 2019).

for these purposes – actions that cause or can cause catastrophic physical damage to facility assets and systems. In December 2013, a former avionics technician entered a secure gate at the Wichita airport using a valid employee access card and attempted to detonate a car bomb. He later pled guilty to one count of use of a weapon of mass destruction – a federal terrorism charge – only because his well-documented ties to violent jihad very clearly revealed a transnational element in the fact pattern of the case (DOJ, 2015).

Now imagine the following scenario: the largest refinery in the United States at Port Arthur, TX undertakes a turnaround to repair a major process unit. In these instances, the regular permanent staff of approximately 1,450 might double to include contractors, temporary help, and outsourcers. A turnaround is a major security risk in and of itself. The regulatory framework exists to help mitigate these risks through certain measures within the Department of Homeland Security's (DHS) Chemical Facility Antiterrorism Standards (CFATS) and the Transportation Safety Administration's (TSA) Transportation Worker Identification Card (TWIC) system, but there are significant flaws in both of these programs.[5] Even so, one contractor with a hidden political agenda whose background check failed to detect any terrorist affiliations or criminal history, with authorized temporary access to a refinery or chemical facility's operational technology (OT) could, with relative ease, facilitate a devastating event that does not involve an explosive device like a car bomb. Such a situation may seem unrealistic, but it is not. Although asset owners and operators do their best in good faith to comply with regulations to manage these security and safety risks, the sheer volume of employees in large turnaround-type situations creates a statistical advantage for the lone assailant. Nonetheless, depending upon the type of attack, such as disabling OT controls to cause a noxious chemical leak versus use of an improvised explosive device, the crime itself may not be prosecuted under federal terrorism laws.

As illustrated, just one person can cause an incident at a critical infrastructure facility, and this is particularly true for cyberattacks. The Department of Energy (DOE) and DHS are actively conducting outreach to educate stakeholders on the ramifications of cyber intrusions on physical security and safety. It is well known that hackers can steal sensitive data with relative ease (Yahoo, 2013 and 2014; Target, 2013; Marriot, 2018; Facebook, 2019; Capital One, 2019; Ecuador, 2019, among others), and remarkably, these reported data breach incidents are occurring with increasing frequency. In addition to sensitive data, a hacker can also access and manipulate ICSs in the United States. A couple of young computer scientists readily demonstrated this by hacking into a 2014 Jeep from more than 10 miles away and remotely taking over the controls (Greenberg, 2015). Certainly, a nuanced hacker with targeted phishing campaigns to a facility's third party suppliers knows how to capitalize on that access to open gates, shut valves, and bridge both the information technology (IT) and OT systems so it becomes possible not to recognize that an attack is occurring until an explosion happens.

Cyberattacks are such a powerful tool that they are increasingly used as part of the United States' military strategy (Schneider, 2019). Still, given that the U.S. is inextricably tied to the global communications infrastructure, the nation's own vulnerabilities are countless. In the critical infrastructure world, companies work tirelessly to uncover and correct these vulnerabilities before they are exploited. Even so, cybersecurity cannot really be guarded by prescriptive regulations

[5] Chief among these concerns is the failure of distinct government agencies to understand these regulatory programs and their risks. For example, a 2019 Department of Justice Office of Inspector General Report noted that 214 terrorist watchlisted individuals applied for a TWIC through FBI between 2006-2017, and some were issued. The TWIC is required by law for unescorted access to secure areas on ports and docks, which many critical infrastructure facilities have on site (DOJ, 2019b, 10).

because innovation is stifled and adaptation in response to new attack vectors is limited. Technologies spread quickly. Within the last 40 years, the world shifted from mainframes to desktops to laptops to mobile devices, then the cloud, and now the "Internet of Things" (Danzig, 2014, 2018). Terrorists, domestic and foreign, exploit these rapid advancements. Acting Director of National Intelligence (DNI) Joseph Maguire recently called attention to this very issue, observing that: "At one point in time, you had to be a sovereign nation to have this kind of technology, but with the proliferation of technology and with the global economy, much of it is now easy to acquire and simple to use" (Cruickshank and Dodwell, 2019, 2011).

Not only is cyberterrorism challenging to attribute, but it is not defined anywhere in the federal criminal code. This is a recognized problem, both for purposes of understanding what constitutes cyberterrorism and for prosecuting offenders. Acting DNI Director Maguire continues, "[Terrorists] use the internet and encryption to a great extent. They understand technology. We are a technological nation, and we have to make sure we understand the problem set and not be reactive but be anticipatory to what they're going to do" (Cruickshank and Dodwell, 2019, 12). As cyberattacks continue to increase and become more sophisticated, safeguarding against cyberterrorism is no longer exclusively a matter of ensuring that private industry is equipped with the appropriate tools to mitigate the risks. The government must assure its citizens, as well as the owners and operators of critical infrastructure assets, that those who perpetrate cyberterrorism are held accountable.

One final emerging threat to critical infrastructure that is increasingly worrisome is drones. The potential safety hazards and security threats presented by errant or malicious unmanned aircraft systems (UAS) activity and the evolving tactics used by hostile operators are provoking a growing number of efforts by public and private sector entities to address these risks. Not only can drones drop explosives and hazardous substances, but they can also be equipped with weapons, conduct unauthorized surveillance, aid hackers in overcoming physical barriers, and act as kamikaze agents for nefarious actors.

The potential for UAS activity to inhibit or halt operations at critical infrastructure facilities is known, as evidenced by recent disruptions to operations at Gatwick Airport in the United Kingdom (December, 2018), Newark Liberty International Airport (January, 2019), and most recently the attacks on Saudi Arabian oil and natural gas infrastructure (September, 2019). At the root of the challenges with UAS activity is the absence of a meaningful regulatory and legal framework.[6] While a catastrophic act performed by a drone could potentially warrant a terrorism charge against the operator, critical infrastructure owners and operators are severely restricted in their ability to defend against these emerging technologies, creating an enormous security and safety risk for assets and personnel.

Although the majority of documented incidents stem from the group of UAS operators categorized as "careless or clueless," there are operators with potential criminal intent. Like the regulatory hurdles that limit response to the careless and clueless, the current legal framework also poses significant challenges for authorities' response to criminal operators. Indeed, there are

[6] Remote Identity (ID), like a license plate on your vehicles, is a foundational regulation needed for technological solutions to work and the basis for other important rulemakings. Unfortunately, the regulation has been delayed multiple times by the United States Federal Aviation Administration (FAA), and was recently relayed to the White House's Office of Information and Regulatory Affairs (OIRA) for interagency review. Providing the critical infrastructure community, law enforcement, and government with a key tool that can identify and distinguish authorized UAS from those that may pose a safety or security threat greatly advances their ability to respond to and prevent potentially hazardous situations.

numerous provisions in Title 18 that preclude critical infrastructure owners from engaging in UAS detection and mitigation activities including the Wiretap Act (18 U.S.C. §2511), the Pen Register Act (18 U.S.C. §2511), and the Aircraft Sabotage Act (18 U.S.C. §32), just to name a few. Despite the clear proliferation of advanced technology and the increased risk that errant UAS present to critical infrastructure and their surrounding communities, a regulatory and funding framework that empowers local authorities to respond to threats by UAS is lacking. Only four federal agencies have the authority to engage in counter-UAS (C-UAS) actions in the United States,[7] and this authority does not allow for continual C-UAS coverage at critical infrastructure facilities. The absence of C-UAS coverage creates a security gap and leaves the critical infrastructure community in the difficult position of balancing a potential threat with the reality of limited funds and authority to effectively respond.

Recognizing these gaps, Congress provided FAA the statutory framework to allow certain facilities to apply for designation as a UAS no-fly zone. Section 2209 of the FAA Extension, Safety, and Security Act of 2016 (FESSA) directs the Secretary of Transportation to establish a process to allow critical infrastructure owners and operators to petition the FAA Administrator to prohibit or restrict the operation of an unmanned aircraft near a fixed site facility.[8] This provision is invaluable for critical infrastructure operators seeking to ensure that rogue UAS are not flying above or near their facilities. However, as of October 2019, FAA has yet to initiate the rulemaking for establishing this process.

A Path Forward

In the wake of recent mass shootings, Congress renewed its call to examine how the United States can better contend with domestic terrorism before violent acts occur. Notably, two recent draft bills proposed by Sen. Martha McSally (R-AZ) and Rep. Adam Schiff (D-CA) would create a crime of domestic terrorism modeled after the current statutory definition, and would criminalize providing material support and resources to those knowingly carrying out these acts (McQuade, 2019). Also of significance, both bills include attempt and conspiracy provisions that embolden federal authorities to intervene before an attack occurs (McQuade, 2019). Nonetheless, civil rights groups say expanding the label of domestic terrorism in the federal statute violates the First Amendment in many cases and is a prime example of federal overreach. Proponents of legislation argue that a statute can be carefully crafted to protect civil liberties and yet still give federal authorities the tools necessary to investigate and prevent terrorism from within the borders.

These proposed bills envision a more globalized threat landscape in line with today's realities. A domestic terrorism law does not need to be a violation of fundamental freedoms: there is no call for the creation of a "domestic terror organizations" list or for peaceful protestors to be arrested. In fact, both bills specifically cite acts of domestic terrorism as "violent acts" and attacks that inflict damage to property that could result in "serious bodily injury" (McQuade, 2019). The intent of domestic terrorism legislation is not to prosecute sign-wielding activists or subdue a fiery political debate, but rather to provide federal authorities with the tools necessary to proactively address a domestic terrorism event that was not yet envisioned when Title 18 was enacted.

---

[7] These four agencies are the Department of Justice, Department of Defense, Department of Homeland Security, and the Federal Bureau of Investigation.

[8] Appropriate applicants include operators and proprietors of critical infrastructure, such as energy production, transmission, and distribution facilities and equipment, oil refineries and chemical facilities, amusement parks, and other locations that warrant such restrictions. In making such determinations, the FAA Administrator is to consider aviation safety, protection of persons and property on the ground, national security, and homeland security issues.

The creation of a meaningful domestic terrorism statute would empower federal agencies to act swiftly in promulgating regulations that support security for our national critical functions. It would bolster private sector efforts to protect critical infrastructure assets. Perhaps most significantly, a domestic terrorism label would have the important narrative effect of signaling the gravity of these crimes and of delegitimizing political violence. First Amendment concerns can and should be respected; these are not mutually exclusive positions, and the U.S. Constitution will always be the bedrock of the laws of the country. No matter how we get there, the United States can no longer afford to disregard the security risks of the 21st century.

References

Congressional Research Service. "Public Mass Shootings in the United States: Selected Implications for Federal Public Health and Safety Policy." Updated April 16, 2013. https://crsreports.congress.gov/product/pdf/R/R43004.

Cruickshank, Paul and Brian Dodwell. 2019. "A View from the CT Foxhole: Joseph Maguire, Acting Director of National Intelligence." *CTC Sentinel* 12, no. 8 (September 2019): 8-13. https://ctc.usma.edu/view-ct-foxhole-joseph-maguire-acting-director-national-intelligence/.

Danzig, Richard J. "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." Center for New American Security, July 2014. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf?mtime=20161010215746.

Department of Homeland Security. 2019a. "Critical Infrastructure Sectors." Accessed October 11, 2019. https://www.dhs.gov/cisa/critical-infrastructure-sectors.

Department of Homeland Security. 2019b. "National Critical Functions Overview" Accessed October 8, 2019. https://www.dhs.gov/cisa/national-critical-functions-overview.

Department of Justice. 2015. "Kansas Man Pleads Guilty in Plot to Explode Car Bomb at Airport." Office of Public Affairs, June 5, 2015. https://www.justice.gov/opa/pr/kansas-man-pleads-guilty-plot-explode-car-bomb-airport.

Department of Justice. 2019a. "Two Women Charged with Offenses Related to Pipeline Attacks." U.S. Attorney's Office for the Southern District of Iowa, October 2, 2019. https://www.justice.gov/usao-sdia/pr/two-women-charged-offenses-related-pipeline-attacks.

Department of Justice. 2019b. "Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats." March 2019. https://oig.justice.gov/reports/2019/a1918.pdf.

Federal Bureau of Investigation. 2019. "Terrorism." Accessed October 2, 2019. https://www.fbi.gov/investigate/terrorism.

Greenberg, Andy. 2015. "Hackers Remotely Kill a Jeep on the Highway – With Me in It." *Wired*, July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Kriel, Robyn and Paul Cruickshank. 2016. "Source: 'Sophisticated' laptop bomb on Somali plane got through X-ray machine." *CNN*, February 12, 2016.

https://www.cnn.com/2016/02/11/africa/somalia-plane-bomb/index.html.

Levine, Mike. 2019. "7 key questions about the threat of domestic terrorism in America." *ABC News*, August 6, 2019. https://abcnews.go.com/Politics/key-questions-threat-domestic-terrorism-america/story?id=64811291.

Li, Yun. 2019. "Saudi oil production cut by 50% after drones attack crude facilities." *CNBC*, September 24, 2019. https://www.cnbc.com/2019/09/14/saudi-arabia-is-shutting-down-half-of-its-oil-production-after-drone-attack-wsj-says.html.

McGarrity, Michael and Thomas Brzozowski. "The 2019 Threat Landscape to the Fuel and Petrochemical Supply Chains." Presentation, 2019 AFPM Security Conference, Austin, TX, May 1, 2019.

McQuade, Barbara. 2019. "Proposed Bills Would Help Combat Domestic Terrorism." *Lawfare*, August 20, 2019. https://www.lawfareblog.com/proposed-bills-would-help-combat-domestic-terrorism.

Riedman, David. 2017. "The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks." *Homeland Security Affairs* 13, Article 3 (June 2017). https://www.hsaj.org/articles/13976.

Schiano, Chris. 2019. "Two Indicted for Sabotaging Dakota Access Pipeline." *Unicorn Riot*, October 2, 2019. https://unicornriot.ninja/2019/two-women-indicted-for-sabotaging-dakota-access-pipeline-construction/.

Schneider, Jacquelyn. 2019. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran?" *The Washington Post*, October 1, 2019. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/.

Williams, Nia. 2016. "Activists disrupt key Canada-U.S. oil pipelines." *Reuters*, October 11, 2016. https://www.reuters.com/article/us-usa-canada-pipelines/activists-disrupt-key-canada-u-s-oil-pipelines-idUSKCN12B26O.