Chapter 15. Homeland Security

PULL QUOTE: "We continue to worry about international terrorism by groups like [al-Qa'ida] and ISIS, but now the threat from lone actors already here in the U.S. and inspired by those groups, the homegrown violent extremists, that threat is even more acute. . . . At the same time, we are particularly focused on domestic terrorism, especially racially or ethnically motivated violent extremists." – Christopher A. Wray, FBI Director[1]

Introduction of the Issue

In 1965, the first President's Commission on Law Enforcement and the Administration of Justice focused on addressing the causes of crime and delinquency. Although radical violent organizations (e.g., the Ku Klux Klan) had long carried out campaigns of terror and groups such as the Black Liberation Army and the Weather Underground carried out violent attacks later in the 1960s and 1970s, the term "homeland security" was not yet part of the nation's vocabulary. It took the terrorist attacks of September 11, 2001, and the loss of thousands of American lives for law enforcement to focus their efforts on preventing and combating international and domestic terrorism. While definitions vary, the 2010 National Security Strategy defined homeland security as "a seamless coordination among federal, state, and local governments to prevent, protect against and respond to threats and natural disasters."[2]

In the nearly 20 years since 9/11, the threats that face the nation have expanded and diversified. Today, these threats come in many different forms, including foreign terrorist organizations (FTOs), radicalized lone actors, domestic violent extremists, malign influence campaigns by state and non-state actors, cyber and other threats to our national infrastructure, and the targeting of government institutions and national elections.

One of the key findings of the 9/11 Commission Report was that United States intelligence agencies needed to improve their ability to "connect the dots."[3] In the aftermath of 9/11, government agencies have made significant progress in breaking down information barriers, changing their culture, and being more transparent and inclusive. Prior to 9/11, federal agencies shielded rather than shared their information. Now, that information is shared across the intelligence community (IC) and with other federal, state, local, tribal, and territorial law enforcement partners. In the past 20 years, the federal law enforcement community has developed ways to make information more accessible to key stakeholders by producing information at lower classification levels to reach a broader audience.

Another significant change since 2001 was the creation of the Department of Homeland Security (DHS) in 2002, which combined 22 different federal departments and agencies into a unified, integrated cabinet agency.[4] DHS's Office of Intelligence and Analysis equips the Homeland Security Enterprise with the intelligence and information needed to keep the nation safe, secure, and resilient. It also oversees the National Network of Fusion Centers that comprises 80 state and locally owned and operated fusions centers. One mechanism fusion centers use to share information is "the Homeland Security Information Network (HSIN), which is DHS's official system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international, and private sector partners. Mission operators use HSIN to access homeland security data, send requests securely between agencies, manage operations, coordinate safety and security for planned events, respond to incidents, and share the information they need to fulfill

[1] Bridget Johnson, "Wray: Racial Violent Extremism Is a Top Priority for FBI 'on the Same Footing as ISIS,'" Homeland Security Today, February 6, 2020, https://www.hstoday.us/subject-matter-areas/counterterrorism/wray-racial-violent-extremism-is-a-top-priority-for-fbi-on-the-same-footing-as-isis/.

[2] Executive Office of the President of the U.S., *National Security Strategy of the United States* (Washington, DC: Executive Office of the President of the U.S., 2010), 2, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[3] National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: Norton, 2004), 408, https://www.9-11commission.gov/report/.

[4] "About DHS," U.S. Department of Homeland Security, accessed June 22, 2020, https://www.dhs.gov/about-dhs.

their missions and help keep their communities safe."[5]

The federal government made other significant changes to address homeland security after 9/11. The Federal Bureau of Investigation (FBI) shifted its priorities to counterterrorism, counterintelligence, and cyber security.[6] The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) created the role of the Director of National Intelligence (DNI) to serve as the head of the IC, which consists of 17 member agencies. The DNI leads the Office of the Director of National Intelligence (ODNI), another new cabinet-level agency created after 9/11. The ODNI's mission is to lead and support IC integration, deliver insights, drive capabilities, and invest in the future. The ODNI is staffed by officers from across the IC and is organized into directorates, centers, and oversight offices that support the DNI's role as head of the IC and manager of the National Intelligence Program.[7]

Information and intelligence are keys to enhanced coordination. While "homeland security" does not appear in the Johnson commission report, "intelligence" is mentioned 77 times: for example, "Procedures for the acquisition and channeling of intelligence must be established so that information is centralized and disseminated to those that need it."[8] While that sentence was written to address riots, it still pertains to threats the nation faces today and can easily be applied to terrorism and many other facets of homeland security. Notably, the biggest change in American law enforcement over the past 50 years has been recognizing the importance of collaborating at all levels of government and with the communities they serve.

To advance the collective homeland security interests, the commission focused on three critical areas: identifying the nature of the threat, information sharing and partnerships, and hardening vulnerabilities. The recommendations in this chapter are designed to enhance national security; maximize unity of effort across federal, state, local, tribal, and territorial entities; and protect the homeland for future generations.

This chapter focuses on recommendations made to keep the nation safe from terrorism, foreign threats, and other security concerns by strengthening laws, policies, funding, training, awareness, information sharing, and partnerships to secure the nation against vulnerabilities ranging from the Southwest border to cybersecurity infrastructure and soft targets nationwide.

[BEGIN TEXT BOX – DIRECT QUOTE]

Department of Homeland Security Today

It is important to appreciate the great progress that the Department [DHS] has made since it was founded. DHS has adopted a multi-tiered approach to the lines of security we pursue, including aviation security and border security.

By gaining the ability to recognize hostile actors long before they reach our borders, we have made our Nation's border's not our first line of defense, but one of many. We have increased the sharing of information about terrorist threats between the Federal Government and state, local, tribal, and territorial entities, as well as private sector partners. We have protected partners. We have protected America's critical infrastructure and empowered American communities. . . . But our work is not finished. Indeed, this is a pivotal moment in the Department's history, as we explicitly acknowledge, and adapt our tools to properly

[5] "Homeland Security Information Network (HSIN)," U.S. Department of Homeland Security, November 19, 2014, https://www.dhs.gov/what-hsin.

[6] *House Appropriations Subcommittee on Commerce Justice, Science, and Related Agencies: Transformation of the Federal Bureau of Investigation* (September 14, 2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation), https://archives.fbi.gov/archives/news/testimony/the-fbi-transformation-since-2001.

[7] "Who We Are: Organization," Office of the Director of National Intelligence, accessed June 22, 2020, https://www.dni.gov/index.php/who-we-are/organizations.

[8] U.S. President's Commission on Law Enforcement and Administration of Justice, *The Challenge of Crime in a Free Society* (Washington, DC: U.S Government Printing Office, 1967), 119, https://www.ncjrs.gov/pdffiles1/nij/42.pdf.

confront, the threats of today. These threats have become more complex, more interconnected, more intertwined with technological advances, and closer to home. As the threats evolve, we must do so as well.

- Kevin McAleenan, Acting Secretary, Department of Homeland Security, *DHS Strategic Framework for Countering Terrorism and Targeted Violence, September 2019*[9]

[END TEXT BOX]

15.1 Identifying the Nature of the Threat: International and Domestic Terrorism

Background

Nearly 20 years have passed since al-Qa'ida (AQ) operatives attacked the United States on 9/11. Terrorist organizations across the globe like AQ and the Islamic State of Iraq and ash-Sham (ISIS) continue to harbor the intent—and, in some cases, the capability—to harm Americans at home and abroad, despite having been broadly suppressed by counterterrorism operations throughout the Middle East and South Asia.

Equally concerning are their efforts to inspire homegrown violent extremists (HVEs)—mostly over the internet—to conduct terrorist attacks in the United States. This remains a concern for federal law enforcement agencies and their state and local partners. In addition to AQ and ISIS, foreign terrorist organizations use a range of political and terrorist tactics to undermine local governments, conduct attacks, and threaten American interests abroad.

Some domestic violent extremists (DVE) in the United States today can be categorized as racially or ethnically motivated violent extremists (RMVE). This violent extremism covers several types including anti-government/anti-authority, animal rights, environmental, and abortion-related. In 2019, DVE attacks in the United States resulted in the death of 32 individuals, making 2019 the deadliest year in domestic terrorism since the 1995 bombing of the federal building in Oklahoma City that killed 168 individuals.

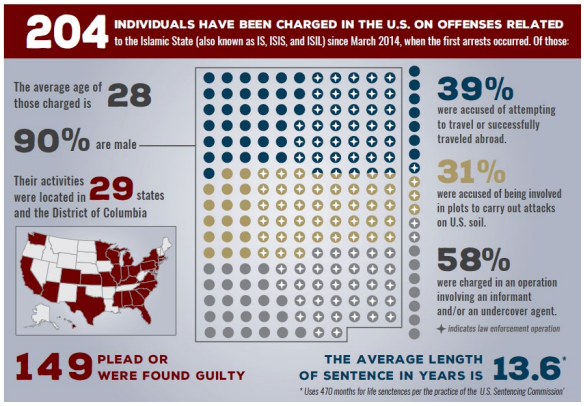
Lone actor violence within the United States has included attacks by violent extremists motivated by international and domestic terrorism. Homeland plotting, foreign travel, and the consumption of terrorist messaging by U.S. based violent extremists who have been inspired by foreign terrorist organizations have evolved significantly since 9/11. Homeland plotting has largely shifted from in-person networks motivated by local radicalizers to self-starting HVEs inspired by overseas ideologues, online radicalizers, and propaganda. Lone actor DVEs affiliated with domestic terrorist ideologies, particularly those associated with racially or ethnically motivated ideology, have become more prevalent, and their actions have become increasingly deadly.

HVEs continue to be inspired by a mix of ideological, sociopolitical, and personal factors. Most successful HVE attackers are radicalized during a period of one to four years and typically mobilized to violence in less than six months, suggesting there may be more time to detect plotters during the radicalization phase than the mobilization phase. In recent years, HVE plotters and attackers have trended younger, underscoring the susceptibility of some adolescents to violent extremist ideologies that appeal to their desire for belonging, identity, or attention. While ISIS continues to be a key influence, it is one of several violent extremist influences that contribute to subjects' radicalization and mobilization. For example, now-deceased ideologue and al-Qa'ida in the Arabian Peninsula senior leader Anwar al-Awlaki, a Yemeni-American jihadist, remains a key influence more than nine years after his death.[10] Since 2014, there have been more than 200 people in

[9] U.S. Department of Homeland Security, *Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence* (Washington, DC: U.S. Department of Homeland Security, 2019), Letter from the Acting Secretary, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[10] Scott Shane, "The Enduring Influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel* 9, no. 7 (2016), https://www.ctc.usma.edu/the-enduring-influence-of-anwar-al-awlaki-in-the-age-of-the-islamic-state/.

the United States charged with offenses related to ISIS.[11]

Like HVEs, DVEs continue to be inspired by a mix of ideological, sociopolitical, and personal factors that vary widely based on individual circumstances. Drivers for most DVEs include perceptions of government or law enforcement overreach, sociopolitical conditions, and reactions to legislation or world events. These trends are primarily enabled by the internet and social media, which facilitates DVEs engaging with others without having to join organized groups. This online communication enables the sharing of literature promoting DVE beliefs, including manifestos and ideologically driven websites that contribute to DVE radicalization. More recently, DVEs are radicalizing based on personalized beliefs that do not correspond with a specific larger DVE threat, but rather a combination of views.



Source: Program on Extremism, The George Washington University, January 2020 Tracker

Current State of the Issue

While combating terrorism and violent extremism is often associated with federal law enforcement agencies that lead the investigations, it is also a local and state problem. Local law enforcement tend to be the first responders, such as the 9/11 attacks or the Boston Marathon bombing. In 2016, the Police Executive Research Forum recognized that "for police agencies and community members alike, violent extremism—which is ideologically motivated violence to further political goals—is a serious and immediate public safety concern."[12] They published *Promising Practices for Using Community Policing to Prevent Violent Extremism* that offers recommendations for a whole-of-government approach that includes planning, training and community outreach and engagement.[13]

In his testimony before Congress, Christopher Wray, FBI Director, says that today, "The top threat we face from domestic violent extremists stems from those we now identify as Racially or Ethnically Motivated Violent Extremists (RMVE). RMVEs were the primary source of ideologically motivated lethal incidents and violence in 2018 and 2019, and have been considered the most lethal of all domestic violent extremism movements since 2001."[14] RMVEs include a wide range of extremists, including most notably those who advocate for the superiority of the White race. According to the New Jersey Office of Homeland Security and Preparedness, "White supremacist tactics indicate members are adopting strategies similar to those employed by foreign terrorist organizations, including strict membership guidelines, online propaganda, and

[11] Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with Homeland Security Working Group, April 6, 2020.
[12] Elizabeth Miller, Jessica Toliver, and David Schanzer, *Promising Practices for Using Community Policing to Prevent Violent Extremism: How to Create and Implement an Outreach Plan* (Washington, DC: Police Executive Research Forum, 2016), 3, https://www.policeforum.org/assets/usingcommunitypolicingtopreventviolentextremism.pdf.
[13] Miller, Toliver, and Schanzer, *Promising Practices*, 3.
[14] *House Judiciary Committee, Hearing on Oversight of the Federal Bureau of Investigation* (February 5, 2020) (statement of Christopher Wray, Director, Federal Bureau of Investigation).

inspiring lone offenders. . . . In June 2018, a self-proclaimed white nationalist created a network called 'The Base,' which shares the English-language name for al-Qa'ida, to promote propaganda [and] encourage violence against minorities."[15]

Another extremist group is sovereign citizens. According to the FBI, "They are anti-government extremists who believe that even though they physically reside in this country, they are separate or 'sovereign' from the United States. As a result, they believe they don't have to answer to any government authority, including courts, taxing entities, motor vehicle departments, or law enforcement."[16] The FBI finds that the greatest threat of violence against law enforcement by domestic extremists stems from those motivated by anti-government extremism, those acting against perceived threats to personal rights, and those acting against perceived unjust policing and judicial systems. Some form of this belief is common to several violent extremist ideologies, including sovereign citizen extremism and militia extremism. Anti-government extremists differ from these other categories in that they do not subscribe to these violent extremist ideologies in total, but often adopt elements of these ideologies, including the use of violence to further their ideology.[17]

In recent years, lethal domestic terrorist attacks have been primarily perpetrated by lone DVEs or by a few DVEs acting without a clear group affiliation or guidance. The current threat is driven by the spread and consumption of ideological content—often First Amendment-protected speech—which is shared across online platforms by DVEs. DVEs also use these platforms to promote potentially radicalizing hate speech and post manifestos outlining grievances. Racial or ethnic minority groups, religious groups, law enforcement, and government personnel and facilities are often the primary targets. Most recent DVE attacks have been intended to inflict mass casualties against soft targets with easily acquired weapons, predominantly firearms. The law enforcement community continues to be challenged by the individualized nature of the radicalization and mobilization processes and the difficulty of distinguishing between violent rhetoric and actual terrorist intent. According to the FBI, out of 22 attacks with 79 fatalities from June 2015 to December 2019, racially or ethnically motivated violent extremists who advocated for the superiority of the White race were responsible for 11 of those attacks, resulting in 52 fatalities.[18]

On the international front, despite enduring the loss of Usama bin Laden and other senior leaders, AQ's global network remains resilient. Its global affiliates continue to plan and carry out terrorist attacks against U.S. interests and allies overseas, while seeking new avenues to inspire or conduct attacks on U.S. soil. As American military deployments in historic AQ safe havens abate, the nation must find ways to enable foreign partners through capacity building and direct assistance. That, in turn, requires new strategies to collect intelligence on the group's plans and capabilities. These strategies will increasingly rely on strong collaboration with foreign partners, local law enforcement, and a more sophisticated understanding of how and where AQ operates online.

As with AQ, disrupting ISIS activities is becoming more dependent on the capacity building of and two-way intelligence sharing with international partners. It also relies on cooperation among domestic and international law enforcement and private sector partners. The keys to preventing the group's resurgence and disrupting its actions are the collective partners' ability to disrupt ISIS's attempts to inspire or enable HVEs and other supporters in the United States and abroad.

---

[15] New Jersey Office Homeland Security and Preparedness, *White Supremacist Extremists Exploit Jihadist Tactics* (n.p.: New Jersey Office of Homeland Security and Preparedness, 2019), https://www.njhomelandsecurity.gov/analysis/white-supremacist-extremists-exploit-jihadist-tactics.

[16] "Domestic Terrorism: The Sovereign Citizen Movement," Federal Bureau of Investigation, April 13, 2010, https://archives.fbi.gov/archives/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement.

[17] (U//FOUO) Federal Bureau of Investigation, U.S. Department of Homeland Security, and National Counterterrorism Center, "Targeting of Law Enforcement by Domestic and Homegrown Violent Extremists," *Joint Intelligence Bulletin*, October 12, 2018.

[18] (U//LES) Federal Bureau Investigation, "Counterterrorism 2020: Domestic Terrorism Threat Overview" (PowerPoint presentation, Washington, DC, April 2020).

As the threats to this country continue to evolve, advances in technology have made it easier for adversaries to communicate and share information via social media and mobile devices.[19] Unfortunately, law enforcement is hindered in its ability to leverage those tools for investigative purposes.[20]

Many of these recommendations transcend both international and domestic terrorism threats. Implementing these recommendations will better position the federal government and its local, state, tribal, territorial, and private sector partners to prevent and mitigate threats of targeted violence.

15.1.1 Congress should enact legislation that ensures federal agencies have access to publicly posted data that is equal to the access provided to commercial entities.

To efficiently search social media platforms for publicly available identifiers of suspected criminals, law enforcement entities use the same automated application programming interfaces (APIs) and access points that non-governmental entities routinely use for commercial and other purposes. These APIs allow law enforcement to perform automated searches across multiple platforms. When properly used, such tools help law enforcement conserve public resources and accelerate investigations, which enhances their ability to identify criminals and bring them to justice.

Over the past few years, social media companies have added language to the terms of service that prohibits law enforcement from using APIs to develop tools to obtain information that is otherwise available to the public on their services. These companies have also added language that prohibits third parties from providing information obtained through the use of APIs to law enforcement agencies. At the same time, these companies allow third parties to use their APIs to collect such information for other reasons, like monetizing the data and marketing goods and services.

Actions by social media companies in this environment reflect a growing trend. Social media companies, rather than elected officials, determine what information and technology law enforcement and public safety officials can use. In essence, decisions that have traditionally been made by elected officials are now being made by corporate officials. Law enforcement operates under the rule of law, abiding by the proper constraints and authorizations set forth by the Constitution and congressional action. The type of information law enforcement seeks is routinely provided to—and exploited by—others. Denying equal access to law enforcement authorities delays the time it takes to identify and stop criminal offenders. In many cases, when law enforcement is denied use of information made public by these companies, additional victimization occurs and law enforcement is forced to expend its limited resources. As a result, some victims may not be identified, and the perpetrators of the crimes against them may never be brought to justice.

The proposed legislation should prevent social media companies from excluding government agencies or their agents from assembling, reviewing, and exploiting publicly posted data if they allow other entities (e.g., marketers) to access and analyze the data. With this access, law enforcement would be able to detect and prevent terrorism, radicalization, and other criminal acts of violence before they occur and without compromising privacy interests.

15.1.2 The Department of Justice, the Department of Homeland Security, and the National Counterterrorism Center should produce an annual report for the public to increase awareness of terrorist threats and encourage public support of counterterrorism efforts.

The public's understanding of the terrorism threat is increasingly integral to law enforcement efforts. Lone actors tend to select targets of opportunity or personal significance, which are difficult for law enforcement to identify and protect prior to an attack. This unpredictability in target selection reinforces the importance of threat awareness and education for not only law enforcement across federal, state, local, tribal, and territorial levels, but also for private sector partners and the public. In addition, law enforcement's ability to

[19] Debra Anderson, Unit Chief, Domestic Terrorism Analysis Unit, Federal Bureau of Investigation, and Seamus Hughes, Deputy Director, Program on Extremism, George Washington University, in discussion with Homeland Security Working Group, April 6, 2020.
[20] David Bowdich, Deputy Director, Federal Bureau of Investigation, in discussion with Homeland Security Working Group, May 7, 2020.

identify and disrupt lone actors has recently been impeded because law enforcement has not been able to access encrypted communications. These limitations have increased the need for bystanders (e.g., family members, peers, community leaders, and strangers) to notice and report concerning changes in behavior before violence occurs. Regardless of whether law enforcement gains access to communications, it is better to have an informed public about potential threats and how they can help identify warning signs. The nation is stronger when law enforcement and an informed public work together.

15.1.3 The Department of Justice, the Department of Homeland Security, and the National Counterterrorism Center should produce an annual terrorism threat assessment to better inform state, local, tribal, and territorial law enforcement officials of current threats.[21]

The terrorism threat has significantly evolved since the attacks of 9/11. Known terrorists are now more likely to be homegrown, self-radicalized actors rather than formal members of FTOs. These homegrown violent extremists, together with racially or ethnically motivated violent extremists, pose a distinct threat to law enforcement because they are often lone actors with easily acquirable weapons who attack soft targets.

The unpredictability in target selection, particularly regarding lone actors, reinforces the importance of threat awareness and education, especially for state, local, tribal, and territorial law enforcement authorities. An annual assessment would provide a look at how terrorism threats have morphed over the prior year and warnings for potential future threats.

The nation faces significant challenges. The Department of Justice (DOJ), the DHS, and the National Counterterrorism Center will continue to adapt ahead of evolving threats by implementing a whole-of-society approach that empowers its citizens; state, local, tribal, and territorial authorities; and private sector, non-governmental, and community leaders. It will also enhance the safety of the nation by producing an annual threat assessment that will help inform federal, state, local, tribal, and territorial law enforcement and private sector partners. DHS notes, "A common baseline understanding of threats within the nation will support interagency policymaking, agency prioritizations, resource allocations, and inter-governmental partnerships."[22]

15.1.4 The National Institute of Justice, in coordination with U.S. Probation and Pretrial Services, should research and develop best practices on supervising ex-inmates who were convicted of crimes relating to radical ideologies. These best practices should be disseminated to local, state, tribal, and territorial authorities.

The National Institute of Justice, in partnership with U.S. Probation and Pretrial Services, should leverage their research, data, and experience to develop and share best practices for state authorities to supervise and monitor former inmates who served time for crimes related to radical ideologies, or served time for other charges but have known affiliations with radical ideologies. This special population requires tailored supervision to help ensure they do not inflict harm based on their radical beliefs. By leveraging research and disseminating best practices, local officials will be better informed and prepared if these individuals are released in their communities.

15.1.5 The White House should issue a National Security Presidential Memorandum aimed at strengthening and synchronizing terrorism and targeted-violence prevention programs across the nation.

Recently, several federal agencies, including the Department of Homeland Security (DHS) and the Federal Bureau of Investigation, have recognized the need to focus more on preventing terrorist and other targeted violence attacks, but no unifying guidance from the White House exists. As a result, state, local, tribal, and territorial law enforcement agencies are left to bridge prevention gaps using their own authority and

[21] This recommendation complements Objective 1.1: Conduct in-depth analysis of current and emerging threats, and share with the homeland security enterprise, from U.S. Department of Homeland Security, *Department of Homeland Security Strategic Framework,* 13–15.
[22] U.S. Department of Homeland Security, *Department of Homeland Security Strategic Framework*, 14.

resources. A national security presidential memorandum (NSPM) may provide the unifying guidance needed to strengthen and synchronize terrorism and targeted violence prevention efforts across the nation.

DHS recently provided $10 million in grants to support the development of prevention capabilities at the local level.[23] Attorney General Barr directed the DOJ to implement national prevention and early engagement programs across the nation.[24] In addition, DHS established the Office for Targeted Violence and Terrorism Prevention. These efforts can support and complement a NSPM that provides much-needed guidance to state, local, tribal, and territorial law enforcement agencies.

Over the past few years, the nation has endured numerous targeted violence attacks, many of which lacked any discernable ideological driver. According to the U.S. Secret Service, 27 mass attacks were carried out in public spaces in the United States in 2018, killing 91 people.[25] In 2017, 28 mass attacks claimed 147 lives, including the deadliest mass attack in modern history: on October 1, a gunman opened fire on the crowd at a music festival in Las Vegas, Nevada, killing 58 people and wounding 546 and leaving a devastating impact on our nation.[26]

The solutions needed to proactively identify, assess, and prevent terrorist and other targeted violence attacks are similar; however, these solutions are applied disparately nationwide. In cases where ideological drivers are known or assumed, the FBI's JTTFs are involved. In cases where ideological drivers are not known or assumed, local law enforcement agencies with varying degrees of experience and capability may become involved. In some cases, no law enforcement agency will be involved until a crisis occurs. Such inconsistency impedes detection and assessment and decreases the likelihood of successful prevention exponentially.

Terrorism is just one form of targeted violence; having a NSPM that provides guidance to preventing such attacks, whether it is a terrorist attack, mass shooting, or school violence would enable agencies to better thwart these types of attacks.[27]

15.1.6 Congress should enact legislation that makes acts of domestic terror a violation of federal law.

Currently, there is no specific federal statute that criminalizes acts of domestic terror. In the absence of such a statute, federal authorities must rely heavily on the use of local and state charges and are compelled to use substitute charges (e.g., civil rights, firearms, and weapons of mass destruction statutes) to prosecute defendants who have carried out domestic terror attacks. A statute modeled on existing statutes that criminalize foreign terrorist activities would provide an important weapon in the fight against domestic terrorism by aiding in investigative efforts, particularly against those who use the internet to radicalize online. This statute should also be crafted to ensure the protection of civil rights and civil liberties.

Profiles of Individuals Radicalized in the United States

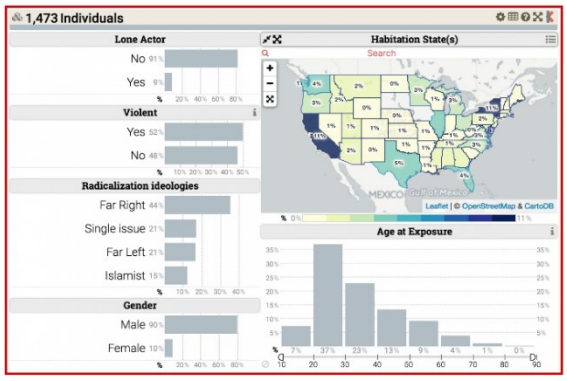
[23] "DHS Makes $10 Million in Funding Available for Targeted Violence and Terrorism Prevention Grants," U.S. Department of Homeland Security, April 21, 2020, https://www.dhs.gov/news/2020/04/21/dhs-makes-10-million-funding-available-targeted-violence-and-terrorism-prevention; and "Targeted Violence and Terrorism Prevention Grant Program," U.S. Department of Homeland Security, accessed July 15, 2020, https://www.dhs.gov/tvtpgrants.

[24] William P. Barr, "Implementation of National Disruption and Early Engagement Programs to Counter the Threat of Mass Shootings" (official memorandum, Washington, DC: U.S. Department of Justice, 2019), https://www.documentcloud.org/documents/6509496-Attorney-General-Memo-Implementation-of-National.html.

[25] U.S. Secret Service National Threat Assessment Center, *Mass Attacks in Public Spaces - 2018* (Washington, DC: U.S. Department of Homeland Security, 2019), 1, https://www.hsdl.org/?view&did=826876.

[26] U.S. Secret Service National Threat Assessment Center, *Mass Attacks in Public Spaces - 2017* (Washington, DC: U.S. Department of Homeland Security, 2018), 7, https://www.secretservice.gov/forms/USSS_NTAC-Mass_Attacks_in_Public_Spaces-2017.pdf.

[27] The Homeland Security Working Group recommends that if the White House issues a national security presidential memorandum, it should leverage existing frameworks and guides such as the U.S. Department of Homeland Security, *Department of Homeland Security Strategic Framework*; Molly Amman et al., *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks* (Washington, DC: Federal Bureau of Investigation, n.d.), https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view; U.S. Department of Justice's Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan* (Washington, DC: U.S. Department of Justice, 2002), https://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf; and Federal Bureau of Investigation, *National Information Sharing Strategy* (Washington, DC: Federal Bureau of Investigation, 2011), https://fas.org/irp/agency/doj/fbi/infoshare.pdf.



Source: National Consortium for the Study of Terrorism and Responses to Terrorism

15.1.7 State, local, tribal, and territorial law enforcement should voluntary track and share their domestic terrorism incidents with the Federal Bureau of Investigation.

With no formal tracking requirements in place to gather data about domestic terrorism incidents from state, local, tribal, and territorial law enforcement, the collection of domestic terrorism incidents should be added to information received from the more than 18,000 law enforcement agencies who voluntarily participate in the FBI's Unified Crime Report (UCR) program. The data should be submitted through a state UCR program or directly to the federal UCR program, and it should be included in the National Incident-Based Reporting System (NIBRS) beginning in 2021.

[CROSS REFERENCE DATA AND REPORTING]

15.2 Information-Sharing and Partnerships

Background

Historically, law enforcement agencies have been hesitant to share information outside the confines of their own organizations. The 9/11 Commission Report highlighted this, noting, "The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is human or systemic resistance to sharing information."[28] That hurdle no longer remains a significant barrier. Since 9/11, law enforcement has dramatically changed how it operates. Federal, state, local, tribal, and territorial law enforcement agencies recognize they are stronger when they work together. As a result, they have prioritized cultivating partnerships with each other, the private sector, and the community. These strengthened partnerships have led to more transparency and an increase in information sharing through such platforms as the FBI Law Enforcement Enterprise Portal and the DHS Homeland Security Information Network.

The federal government cannot connect the dots without the help of state, local, tribal, and territorial communities, and vice versa. The National Network of Fusion Centers (the Network) comprises 80 fusion centers across all states and territories that are owned and operated by state and local entities, with support from federal partners.[29] They facilitate two-way intelligence and information flow among the federal government; state, local, tribal, and territorial agencies; and private sector partners. Fusion centers conduct analysis and facilitate information sharing by assisting law enforcement, fire, public health, homeland security, emergency management, and private sector critical infrastructure partners in preventing, protecting against, and responding to crime and terrorism. The Network plays a critical role in enhancing the nation's

[28] National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission*, 416.
[29] "National Network of Fusion Centers Fact Sheet," U.S. Department of Homeland Security, accessed June 23, 2020, https://www.dhs.gov/national-network-fusion-centers-fact-sheet; Rachel A. Seitz, Enterprise Performance and Evaluation, U.S. Department of Homeland Security, email communication with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, May 8, 2020; and Alberto Martinez, Deputy Director, Orange County Intelligence Assessment Center, CA, in discussion with Homeland Security Working Group, April 13, 2020.

ability to support public safety and counterterrorism missions. They also assist in federal investigations.

With regard to the private sector, many entities have partnered with federal agencies to share critical data related to travel and global supply chains.[30] The FBI, DHS, and ODNI all established offices focused on partner engagement that work closely with state, local, tribal, and territorial law enforcement, fusion center partners nationwide, and private sector partners.[31] DHS established the Public-Private Analytic Exchange Program that enables U.S. government analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary, roles can operate in tandem to ensure mission success. Participants work to create unclassified joint analytic deliverables of interest to both the private sector and the federal government. This program focuses on such topics as cyber resilience and response, emerging technologies and national security, and vulnerabilities of health care IT systems.[32]

Source: DHS Office of Intelligence and Analysis, Office of State and Local Partner Engagement

Current State of the Issue

Since the Johnson report, the United States has built a strong intelligence and information-sharing capability. That capability was enhanced considerably after 9/11, which included establishing fusion centers; issuing security clearances to state, local, tribal, and territorial law enforcement personnel based on their roles and responsibilities in assisting the federal government to fight terrorism; expanding access to classified systems in state and local agencies; and declassifying information to make it accessible at the "law enforcement sensitive" or "for official use only" classification levels, thus allowing critical information to reach a broader law enforcement audience. These efforts focus on sharing knowledge and information with as many partners as possible, because such dissemination is vital to prevent and mitigate harm.[33]

[30] Roland Suliveras, Executive Director, National Targeting Center-Cargo, U.S. Customs and Border Protection, in discussion with Homeland Security Working Group, April 27, 2020.

[31] Sarah Chervenak, Unit Chief, Office of Partner Engagement, Federal Bureau of Investigation, and Russ Porter, Chief of Strategic Partnerships, National Counterintelligence and Security Center, Office of the Director of National Intelligence, in discussion with Homeland Security Working Group, April 13, 2020; and Alethea Madello, Acting Director, and Susan Bower, State and Local Partner Engagement, Office of Intelligence and Analysis, U.S. Department of Homeland Security, in discussion with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, May 1, 2020.

[32] Brian Murphy, Principal Deputy Undersecretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security, in discussion with the Homeland Security Working Group, April 27, 2020; and "2020 Public-Private Analytic Exchange Program," U.S. Department of Homeland Security, accessed July 31, 2020, https://www.dhs.gov/sites/default/files/publications/2020_aep_program_overview_508.pdf.

[33] Russ Porter, Chief of Strategic Partnerships, National Counterintelligence and Security Center, Office of the Director of National Intelligence, in discussion with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, April 17, 2020.

While numerous partnerships have been cultivated, Steven Mabeus, Assistant Director of National Intelligence, is concerned that they are "generally personality-based, threat-related, and regional in scope."[34] Recognizing this as a potential weakness, many government agencies focus on institutionalizing sustainable partnerships rather than being dependent on individualized relationships. Examples include the Global Advisory Committee, Criminal Intelligence Coordination Council, the Homeland Security Advisory Council, the National Counterterrorism Center's Joint Counterterrorism Assessment Team, and the DNI's Homeland Security and Law Enforcement Partners Board.

Law enforcement agencies at all levels of government have established robust partnerships with each other and other key stakeholders in the private sector, the community, and abroad. Still, more can be accomplished to connect the dots through partnerships and information sharing.

[BEGIN TEXT BOX – DIRECT QUOTE]

Information Sharing

Terrorism is terrorism. . . . We do not and cannot fight this battle alone. Our people are collaborating and communicating at a high level in Joint Terrorism Task Forces across the country and also within the numerous Fusion Centers throughout the nation.

In my career I have worked with many Fusion Centers, to include some in your districts, and the work we're doing together there is simply amazing. In fact, information provided by the Fusion Center in Orange County, California, led us to predicate cases that recently resulted in seven arrests of members of The Base across four different states. Collectively, we are working around the clock to push out real-time intelligence to federal, state local, tribal, and territorial agencies.

This collaboration will continue to be vital as we face new trends in the threat.[35]

- Jill Sanborn, FBI Assistant Director of the Counterterrorism Division, Testimony on Confronting the Rise of Anti-Semitic Domestic Terrorism, February 26, 2020

[END TEXT BOX]

15.2.1 Congress should authorize and appropriate annual funding for the Department of Justice and the Department of Homeland Security to enable federal law enforcement agencies to establish full-time positions at all primary and recognized fusion centers that comprise the National Network of Fusion Centers.

The National Network of Fusion Centers (the Network) represents a shared commitment between the federal government and the state and local governments that own and operate the fusion centers. Individually, each is a vital resource for collecting, analyzing, and integrating national, state, and local all-crimes, all-hazard information and making it relevant to their partners to prevent and respond to all threats and hazards.[36] The Network provides critical investigative support to DOJ and DHS investigations by providing key local data and case support. Federal partners that assign personnel to fusion centers gain first-hand access to all of the established state and local relationships each fusion center has. They can also access local databases that they would not otherwise be able to access.

Anecdotal evidence shows that fusion centers benefit from federal personnel being co-located at a fusion center. Director Chris Hayes and Deputy Director Alberto Martinez from the Orange County Information Assessment Center (OCIAC) both echoed the value of having federal employees, including those from the FBI

[34] Steven Mabeus, Deputy Director, Office of the Director of National Intelligence, public comment to Homeland Security Working Group, April 30, 2020.
[35] *U.S. House Subcommittee on Intelligence and Counterterrorism: Hearing on Confronting the Rise of Anti-Semitic Domestic Terrorism, Part II, 116th Congress* (February 26, 2020) (statement of Jill Sanborn, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation).
[36] "Fusion Centers," U.S. Department of Homeland Security, September 19, 2019, https://www.dhs.gov/fusion-centers.

and DHS, embedded in the OCIAC; this co-location is what makes the OCIAC strong.[37] According to the DHS's Office of Intelligence and Analysis in 2019, the FBI had approximately 90 personnel in 38 fusion centers, and DHS had 95 personnel embedded in fusion centers.[38] However, the number of personnel is considerably less among other federal law enforcement agencies. The Bureau of Alcohol, Tobacco, Firearms, and Explosives has 12 employees working in fusion centers, and Immigration and Custom Enforcement (ICE) has nine employees in fusion centers. The DEA, the Transportation Security Agency, CBP, and the Federal Law Enforcement Training Center all have either one or two representatives.[39]

The Network was established and evolved as a response to the 9/11 intelligence failures. Yet, without specific appropriated funding, federal law enforcement agencies have not been able to dedicate the needed personnel to enhance fusion centers. In 2016, based on a Congressional Directed Action from the Senate Select Committee on Intelligence, the FBI was ordered to staff 66 positions at the National Counterterrorism Center (NCTC).[40]

The commission recommends congressional action to staff federal personnel at fusion centers, similar to the NCTC Congressional Directed Action. Doing so will increase the number of federal agencies that will be able to deploy personnel to fusion centers. Fusion centers require the cooperative efforts of various member agencies to provide a mix of skills, experience, and enforcement jurisdiction which no single agency possesses. The Network's strength is its ability to draw upon the combined skills, expertise, and techniques of each participating agency, including federal law enforcement agencies.

[CROSS REFERENCE GRANTS]

15.2.2 Congress should authorize and appropriate funding for a dedicated Department of Homeland Security fusion center grant program that provides funds directly to states and local jurisdictions that operate primary and recognized fusion centers comprising the National Network of Fusion Centers.

[CROSS REFERENCE GRANTS]

The Network brings critical context and value to homeland security and law enforcement partners. Fusion centers accomplish this through sharing information, providing partners with a unique perspective on threats to their state or locality, and being the primary conduit between frontline personnel, state and local leadership, and the rest of the homeland security enterprise. However, there is no dedicated funding program to sustain and support these ongoing collaboration and information-sharing efforts. Fusion centers receive operational funding from federal (through both grants and direct contributions), state, local, tribal, territorial, and private sector sources.[41]

Currently, most fusion centers receive funding through the Federal Emergency Management Agency (FEMA) Preparedness Grant Program, specifically the State Homeland Security Grant Program and the Urban Area Security Initiative. These funds represent varying percentages of overall fusion center budgets, with some centers mostly funded by state or local governments and other centers mostly funded through federal grants.

There is no certainty from one year to the next that a particular fusion center will receive funding that is adequate to build and sustain analytical, information sharing, and liaison capabilities to fulfill their missions and support local, state, and federal priorities. This uncertain support does not match the essential nature of the work that fusion centers perform. In addition, the current grant process pits law enforcement against

[37] Chris Hayes, Director, and Alberto Martinez, Deputy Director, Orange County Intelligence Assessment Center, CA, in discussion with Homeland Security Working Group, virtual site visit to the Orange County Intelligence Assessment Center, April 16, 2020.
[38] Seitz, email communication to Amy Schapiro, May 8, 2020.
[39] Seitz, email communication to Amy Schapiro, May 8, 2020. Data for personnel assigned from federal agencies are derived from a U.S. Department of Homeland Security Office of Intelligence and Analysis Federal Cost Inventory (annual data call). Data received are based on whether they receive responses from those components or agencies. These data are based on responses to the 2018 Federal Cost Inventory.
[40] Intelligence Authorization Act for Fiscal Year 2016, H.R. 2596 114th Cong, (2015); (TS//SCI; information used in this report is unclassified) *FY16 Intelligence Authorization Act Annex* (Washington, DC: Government Printing Office, 2016).
[42] U.S. President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime*.

emergency management and other state stakeholders for funding intended for terrorism and violence prevention. As a result, consistent funding of critical prevention capabilities is not ensured. A dedicated fusion center grant stream would ensure that all primary and recognized fusion centers can plan, build, and maintain capabilities that are essential to their missions.

15.2.3 The Department of Homeland Security and the Federal Bureau of Investigation should provide intelligence training to state and local authorities that focuses on integrating criminal intelligence with national intelligence to better protect the nation.

The Johnson commission emphasized the importance of participation and coordination among federal, local, state, and private groups to address the problems at hand, and that sentiment has not changed. In 1967, the focus was on organized crime and corruption.[42] Today, it is terrorism and security. The need to have informed leadership making critical decisions remains constant.

The Johnson commission recommended that law enforcement officials provide regular briefings to leaders at all levels of government concerning relevant conditions within each jurisdiction. The training proposed by this commission ensures that local leaders are briefed and understand the criminal and intelligence threat pictures.

By providing a fuller understanding of the information and intelligence landscape through training, state and local authorities will be better positioned to understand potential threats that can have an impact on their decision-making. This training should also provide an understanding of the capabilities of their local fusion centers.

15.2.4 The Intelligence Community should develop a unified strategy to increase awareness of foreign influence threats that have an impact on state and local jurisdictions and the private sector.

Today's complex counterintelligence threat requires a whole-of-society approach. Nation-state actors attempt to exploit America’s economy, technology, information, and the rule of law, threatening national and economic security. The law enforcement community is actively targeted by foreign adversaries seeking to compromise sensitive law enforcement information and databases and to influence law enforcement partners for malign purposes. Therefore, the federal government should raise awareness about these threats by sharing information and intelligence more widely. A particular focus should be on non-terrorist threats posed to homeland security, such as those advanced by well-financed, highly organized, and sophisticated foreign intelligence adversaries and their proxies who use social media and other platforms to drive division. The federal government should leverage the post-9/11 terrorism-related information-sharing structures and processes to broaden information sharing to include foreign intelligence threats and to share relevant information with a wider range of recipients (e.g., governors; mayors; or heads of state, local, tribal, and territorial government entities). Organizational structures, such as task forces established by the FBI, should be prioritized.

Additionally, federal agencies should implement similarly constructed internal task forces to bridge agency responsibilities to reduce redundancy and better incorporate information sharing efforts that mitigate today’s counterintelligence threat. The establishment of the FBI’s Foreign Influence Task Force is an ideal standard by which the federal government can synthesize information, coordinate responses, and bring different authorities to mitigate threats. Organizational constructs such as task forces can be both permanent or ad hoc to remain agile depending on the nature and scale of the counterintelligence threat.

15.2.5 The Department of Homeland Security should survey state, local, tribal, and territorial law enforcement, fire departments, and other emergency medical services information systems that may be used to improve reporting and analysis of threats of mass casualty attacks and threats to school safety. Special focus should be placed on information systems that can inform behavioral threat assessment

[42] U.S. President’s Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime*.

processes and assist in the threat management process.

By surveying agencies to gather more knowledge about their information systems, the federal government can better leverage those systems to improve the reporting and analysis of mass casualty threats or school shootings. The federal government can also advance both the threat picture and the national suspicious activity reporting initiative by adapting existing processes, systems, and protocol.

15.3 Hardening Vulnerabilities

PULL QUOTE: "A secure border will lead to a more secure nation." – Sheriff Mark Napier, Pima County, Arizona[43]

Background

When discussing how best to strengthen the nation, the commission identified three vulnerabilities that threaten national security: border security, hardening soft targets, and cybersecurity.

The complex issues that border security entails have plagued the country for years. While much attention has been given to fortifying the Southwest border, Sheriff Mark Napier of Pima County, Arizona, framed the issue in a broader content. He views border security as needing a three-tiered approach, addressing public safety, national security, and human rights.[44] While acknowledging the lion's share of attention is focused on drug smuggling, gangs, sex trafficking, human smuggling, and illegal aliens, Sheriff Napier remains passionate that border security must be addressed as a humanitarian issue. He discussed the abuse many illegal aliens experience trying to cross the border, coupled with the unforgiving environmental conditions at the border. He also discussed the financial and emotional toll on law enforcement to process, handle, and move decomposing bodies found in remote and inaccessible areas. Sheriff Leon Wilmot summed the state of the border best: "The lack of a secure border presents a public safety crisis, not only for border counties but also for our nation."[45]

In addition to the bleak picture painted by subject matter experts about border security shortcomings and the impact on national security, another area of concern was the safety and security of the public while attending large and crowded gathering places, such as sports venues, nightclubs, concerts, and movies. Attacks on such places have been seen in the United States, from the Pulse Night Club massacre in Orlando and the Boston Marathon bombing to mass shootings at religious institutions of various denominations in Oak Creek, Wisconsin; Charleston, South Carolina; and Pittsburgh, Pennsylvania.

Such locations are grouped under the term soft targets and crowded places: locations or environments that are easily accessible, attract large numbers of people on a predictable or semi-predictable basis, and may be vulnerable to attacks using simple tactics and readily available weapons.[46]

Jeff Miller, Vice-President of Security for the Kansas City Chiefs, spoke about the multiple risks seen at such venues, ranging from active shooters to critical infrastructure failures. Once these vulnerabilities and their potential consequences are brought to the attention of decision-makers who preside over large venues, they often dedicate the needed funds for hardening their premises.[47] While Mr. Miller spoke in detail about safely securing sports stadiums, he pointed out the similarity of security and safety issues for other large, non-

[43] Mark Napier, Sheriff, Pima County Sheriff's Department, AZ, in discussion with Homeland Security Working Group, April 20, 2020.
[44] Napier, in discussion with Homeland Security, April 20, 2020.
[45] Leon Wilmot, Sheriff, Yuma County Sheriff's Office, AZ, email communication with Amy Schapiro, Federal Program Manager, Homeland Security Working Group, June 1, 2020.
[46] U.S. Department of Homeland Security, *Notice of Funding Opportunity Fiscal Year 2020 Homeland Security Grant Program* (Washington, DC: U.S. Department of Homeland Security, 2020), 3, https://www.fema.gov/media-library-data/1583442273016-07cbcf9445f9fda3cdc5bf8439ec72c9/FY_2020_HSGP_NOFO_FINAL_508ML4.pdf.
[47] Jeff Miller, Vice-President of Security, Kansas City Chiefs, in discussion with Homeland Security Working Group, April 27, 2020.

sports gatherings (e.g., parades) and the attendant vulnerability issues connected to them.

[BEGIN TEXT BOX]

Resources Available for Soft Targets and Crowded Places

The Department of Homeland Security (DHS) recognizes the need to raise awareness about the vulnerabilities inherent in soft targets and crowded places. In their Homeland Security Grant Program, administered by the Federal Emergency Management Agency (FEMA), one of the four prioritized areas includes, "enhancing the protection of soft targets/crowded places."[48] The FEMA grants available to local and state governments to support soft target preparedness activities are the State Homeland Security Program and the Urban Area Security Initiative. Information about both can be found here: https://www.fema.gov/homeland-security-grant-program.

In addition to funding, DHS has several informational resources available, including a guidebook about their efforts entitled *Soft Targets and Crowded Places Security Enhancement and Coordination Plan*, which other agencies can leverage to help protect soft targets and crowded places in their communities.

The DHS Office of Science and Technology has published the fact sheets *Security for Large Crowds and Venues*[49] and *Predicting Crowd Behavior Fact Sheet and Video,*[50] which focus on enabling safer crowd movement during emergencies and other events.

The following publications related to securing large events are available from the Department of Justice Office of Community Oriented Policing Services and the Bureau of Justice Assistance:

Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement

https://cops.usdoj.gov/RIC/Publications/cops-w0703-pub.pdf

Planning and Managing Security for Major Special Events: Training Curricula

https://cops.usdoj.gov/RIC/ric.php?page=detail&id=COPS-CD026

Managing Large-Scale Security Events: A planning Primer for Law Enforcement Agencies

https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/LSSE-planning-Primer.pdf

[END TEXT BOX]

From each attack, new information is gleaned about how to prevent a repeat. For example, the Manchester, England, bombing at an Ariana Grande concert prompted the New York City Police Department (NYPD) to rethink how they secure major events. As NYPD Deputy Commissioner John Miller said, "The event does not end once everyone has entered safely. When people leave, the threat starts again."[51]

Another vulnerability the commission looked at was the need for heightened cybersecurity. As adversaries try to attack the security of this nation, they often attempt to infiltrate and harm cyber infrastructure, which can have damaging effects on our critical infrastructure, democracy, and safety.

Current State of the Issue

[48] U.S. Department of Homeland Security, *Notice of Funding Opportunity Fiscal Year 2020,* 3.
[49] U.S. Department of Homeland Security Science and Technology Center of Excellence, *S&T Security for Large Crowds and Venues Fact Sheet* (Washington, DC: U.S. Department of Homeland Security, 2019), https://www.dhs.gov/publication/st-security-large-crowds-and-venues-fact-sheet.
[50] U.S. Department of Homeland Security Science and Technology Center of Excellence, *S&T Predicting Crowd Behavior Fact Sheet and Video* (Washington, DC: U.S. Department of Homeland Security, 2019), https://www.dhs.gov/publication/st-predicting-crowd-behavior-fact-sheet-and-video.
[51] John Miller, Deputy Commissioner, New York City Police Department, NY, in discussion with Homeland Security Working Group, April 27, 2020.

As this commission report was being developed, the nation was confronted with a new threat: COVID-19. This pandemic has directly affected operations on the Southwest border. In April 2020, the number of illegal migrant encounters at the Southwest border were down 88 percent compared to the year prior.[52] Vehicular and pedestrian crossings were both down, largely because of travel restrictions implemented to slow the spread of the coronavirus. During this time, narcotic seizures were up.[53]

The national security threat the border represents is compounded by how it has evolved since 9/11. The current concern is toward low-tech lone-wolf type attacks, such as physical attacks with hand weapons in crowded areas, suicide bombings, and the weaponization of common vehicles. Leon Wilmot, Sheriff of Yuma County Sheriff's Office, states, "These single bad actors could easily enter the United States undetected through the Southwest border. . . . We have ample evidence of the lethality that a single motivated person can possess through a very low-tech random attack. One of these people entering our country undetected is too many. The lack of border security is an undeniable national security concern."[54]

In addition to the impact of COVID-19, there is concern about cyberattacks threatening the presidential election of 2020 and the constant possibility of attacks on soft targets and in crowded places. Government officials have sounded the alarm about adversaries such as China leveraging their cyber capability to attack the United States. According to the DNI's World Threat Assessment:

> Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.[55]

The Orange County Intelligence Assessment Center in California (OCIAC) offers vulnerability assessments of critical infrastructure, including onsite physical threat assessments, and facilitates briefings with event personnel for mass gatherings. It also shares preventive awareness and DHS information. Recognizing the importance of vulnerability assessments, the OCIAC provides training so other agencies so they can conduct physical threat assessments in the future.[56]

Border Security

15.3.1 Congress should provide additional funding to federal agencies to construct and maintain a comprehensive border security system. This funding should support immigration enforcement detention capacity and space, technological infrastructure, and combined durable physical and technology systems that help secure national borders.

One of the United States' greatest homeland security vulnerabilities is the lack of comprehensive border security. A secure border requires a layered approach that involves multiple stakeholders at federal, state, and local levels; technology; and durable combined physical and technology systems. These systems should include physical barriers where appropriate, sensors, and a fleet of surveillance drones that cover the entire U.S.–Mexico border. These drones would allow authorities to see in real time who and what attempts to cross the border.

To properly manage and secure the border, there must be sufficient immigration enforcement detention capacity to effect the apprehension, detention, and subsequent removal of individuals who enter the United States illegally. These combined tools should provide adequate controls to manage and mitigate illegal

[52] (U//FOUO) Customs and Border Protection, "CBP Weekly Messaging," May 11, 2020.
[53] (U//FOUO) Customs and Border Protection, "CBP Weekly Messaging," May 11, 2020.
[54] Wilmot, email communication with Amy Schapiro, June 1, 2020.
[55] Dan Coats, *Statement for the Record: World Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[56] Greg Fox, Captain, Anaheim Fire and Rescue, CA, in discussion with Homeland Security Working Group, virtual field visit to the Orange County Intelligence Assessment Center, April 16, 2020.

migration flows, which should therefore improve national security and the safety of the American people.

15.3.2 Congress should enact legislation that raises the penalty for illegally entering the United States from a misdemeanor to a felony. This legislation should also clearly state that being in the United States without legal authorization is a continuing offense, and that the statute of limitations does not begin from the time the alien illegally entered the United States.

At present, illegally entering the United States without any aggravating factors is punishable only as misdemeanor (8 U.S.C. § 1325), which applies to asylum seekers but not if they come through a port of entry. This does not sufficiently deter those who are determined to enter the United States illegally, nor does it provide sufficient punishment for those who do. Further, when aliens are found in the United States more than a year after their illegal entry, criminal prosecution may be impossible if courts determine that the one-year statute of limitations began upon the alien's illegal entry.

15.3.3 Congress should enact legislation to codify the authority of state and local law enforcement agencies to briefly maintain custody of prisoners and inmates for whom there is reason to believe they are aliens who could be removable from the United States. These inmates should be delivered to Immigration and Customs Enforcement's custody to face immigration removal procedures after serving their state sentence.

State and local law enforcement partners who are willing to briefly detain alien prisoners and inmates so that Immigration and Customs Enforcement (ICE) can take custody of them face legal jeopardy in some jurisdictions. Implementing this recommendation would lessen the litigation risks that are associated with cooperating with ICE and help secure the nation, as criminal aliens and terrorists who are removable from the United States will be removed according to established immigration laws and procedures.

15.3.4 Congress should enact legislation that authorizes and appropriates the Federal Emergency Management Agency's Operation Stonegarden grant program to provide increased funding for border operations and resources geared for law enforcement agencies along the national border.

[CROSS-REFERENCE GRANTS]

FEMA administers Operation Stonegarden (OPSG), a grant program that supports enhanced cooperation and coordination among CBP, United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies. The OPSG program funds investments in joint efforts to secure the United States borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada and in states and territories that border international water.[57]

As the issues that plague the border intensify, particularly along the Southwest border, law enforcement agencies along the nation's border need increased funding and resources to support operations. Dedicating the appropriated funding for Operation Stonegarden would enable a whole-of-community, counter-network approach to defeat transnational criminal organizations and provide front-line anti-terrorism defense of the nation.

15.3.5 Congress should authorize and appropriate funds to the Department of Justice to establish a grant program tailored to the Southwest border. This program should address the public safety, national security, and humanitarian issues that are prevalent in border communities. This funding should go directly to local law enforcement agencies and not through the state authorities for dissemination.

[CROSS REFERENCE GRANTS]

Local law enforcement agencies along the Southwest border are confronted with challenges unique to their jurisdictions. While their duties focus on protecting and serving the public, there are not many other agencies

[57] "Operation Stonegarden (OPSG) Program," Homeland Security Grants, accessed May 10, 2020, https://www.homelandsecuritygrants.info/grantdetails.aspx?gid=21875.

that confront the same volume of humanitarian issues, which include human smuggling, human trafficking, sex abuse, criminal abuse, transnational criminal organizations, or drug smuggling.

In addition, sheriffs on the Southwest border house illegal aliens who have been charged with state crimes. In Arizona, this leads to approximately $30 million every year in unanticipated costs for housing, feeding, and providing medical care to illegal aliens.[58] Through the Bureau of Justice Assistance's State Criminal Alien Assistant grant program, in partnership with ICE, local agencies are reimbursed for incarcerating undocumented criminal aliens with at least one felony or two misdemeanor convictions for violations of state or local law, and incarcerated for at least four consecutive days during the reporting period.[59] Yet, border sheriffs say this is not enough because the aid provided is equivalent to roughly five cents on the dollar for their expenditures, which does not begin to cover their incurred expenses.[60]

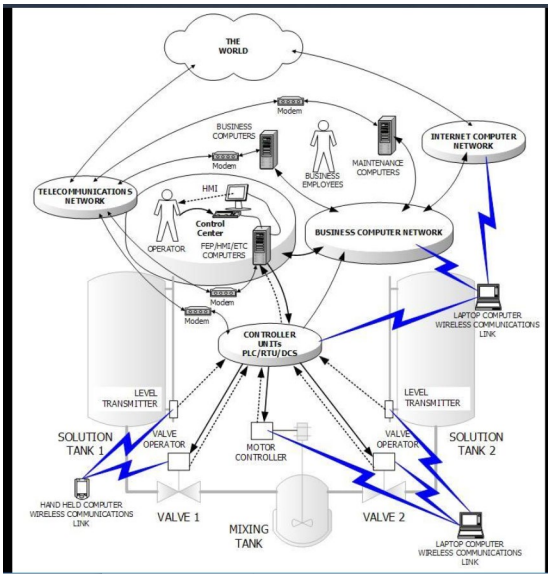
While grants are currently available to agencies along the Southwest border, most funding is disseminated through the state and funneled down to local law enforcement. Administering grants directly to these local law enforcement agencies on the Southwest Border will reduce administrative costs and help streamline the grant-making process. It will also provide needed funds to address the mounting humanitarian, public safety, and national security issues that law enforcement on the Southwest border encounter daily.

15.3.6 The legislative and executive branches should institutionalize a formal mechanism to ensure that border sheriffs and other key local stakeholders help formulate policy decisions that have an impact on the Southwest border.

Border sheriffs and other key officials and stakeholders who are involved in formulating their own policy decisions that have an impact on the Southwest border know their territory and its inhabitants well. They have insight into population flow and have learned to incorporate their collective knowledge to arrive at the most efficacious and humane policy decisions. Their input would be invaluable in any policy decision making that involves federal officials.

Cybersecurity and Soft Targets

Understanding Control System Cyber Vulnerabilities



[58] Leon Wilmot, Yuma County Sheriff's Office, AZ, in discussion with Homeland Security Working Group, April 20, 2020.
[59] "State Criminal Alien Assistance Program Overview," Bureau of Justice Assistance, accessed June 24, 2020, https://bja.ojp.gov/program/state-criminal-alien-assistance-program-scaap/overview.
[60] Mark Dannels, Sheriff, Cochise County Sheriff's Office, AZ, Mark Napier, Pima County Sheriff's Department, AZ, and Leon Wilmot, Yuma County Sheriff's Office, AZ, in discussion with Homeland Security Working Group, April 20, 2020.

Source: U.S. Computer Emergency Readiness Team (U.S. CERT)

15.3.7 The Federal Bureau of Investigation and Department of Homeland Security's Cybersecurity and Infrastructure Agency should inform to state, local, tribal, and territorial government technological procurement offices regarding companies and components known to carry cybersecurity risks.

Some adversaries likely engage in cyber espionage, which includes obtaining cyber information accessible to companies that are operating in their country. It can be difficult for state, local, tribal, and territorial governments to identify companies or technology with ties to these countries due to the number of subsidiaries; the lack of visibility on components and their manufacturers; and the tendency for many commercial, off-the-shelf products to arrive pre-loaded with software. Resources or guidance for procurement officers on how to identify potential vulnerabilities can enable state, local, tribal, and territorial governments to make better technological purchasing decisions, which will protect the nation's cyber infrastructure.[61]