Research Report

JOHN S. HOLLYWOOD, KEITH GIERLACK, PAULINE MOORE,
THOMAS GOODE, HENRY H. WILLIS, DEVON HILL,
RAHIM ALI, ANNIE BROTHERS, RYAN BAUER, JONATHAN TRAN

Improving the Security of Soft Targets and Crowded Places

A Landscape Assessment

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the RAND Corporation under contract with DHS

This research was published in 2024.

About This Report

Attacks on soft targets (STs) and crowded places (CPs) (ST-CPs) represent a significant challenge in the 2023 security environment. The U.S. Department of Homeland Security (DHS) requires research and development support to evaluate methods for reducing the propensity and scale of damage and loss of life from these types of attacks. In response, researchers from the Homeland Security Operational Analysis Center (HSOAC) conducted a comprehensive landscape assessment of the threat to ST-CPs and corresponding security measures by integrating literature reviews, analyzing data on attack plots, reviewing grant data, and modeling security to identify needs for improving security. We then recommended research and investment priorities for addressing those needs. This report should be of interest to the broad ST-CP security community, including site security managers, planners, funders, and governmental personnel with interests in protecting ST-CPs.

This research was sponsored by DHS's Science and Technology Directorate (S&T) and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division, which operates HSOAC.

About the Homeland Security Operational Analysis Center

The Homeland Security Act of 2002 (Public Law 107-296, § 305, as codified at 6 U.S.C. § 185) authorizes the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. The RAND Corporation operates HSOAC as an FFRDC for DHS S&T under contract 70RSAT22D00000001.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. HSOAC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. HSOAC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task order 70RSAT22FR0000074, Soft Target and Crowded Places Landscape Assessment and Research Roadmap. The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information on the RAND Homeland Security Research Division, see www.rand.org/hsrd. For more information on this publication, see www.rand.org/t/RRA2260-1.

Acknowledgments

We would like to thank Ajmal Aziz of the Science and Technology Directorate for his exceptional direction, dedication to advancing public safety, and strong support of this effort. We would also like to thank the subject-matter experts with whom we met during this project, whose expertise has resulted in significant contributions to this effort. The efforts of our own internal experts and advisers—Andrew Lauland, Donell Harvin, and Shoshana R. Shelton—led to major improvements to this work, and we are grateful for their feedback and insights. We would also like to thank the peer reviewers, Heather J. Williams and J. D. Williams, for their insights and recommendations, which also led to significant advances in this report.

Summary

Attacks on soft targets (STs) and crowded places (CPs) (ST-CPs) represent a significant challenge in the 2023 security environment. The U.S. Department of Homeland Security requires research and development to assess methods for reducing the propensity and loss of life from these types of attacks. In response, we conducted a comprehensive landscape assessment of the threat to ST-CPs and corresponding security measures, which integrated literature reviews, attack plot analyses, grant data reviews, and security cost modeling to identify both needs for improvement and recommended research and investment priorities for addressing those needs.

The Attack Threat for Soft Targets and Crowded Places

The threat to ST-CPs is substantially more diffuse than terrorism.[1] The number of attack plots is broadly aligned with regional population counts. The major exceptions have been New York City and Washington, D.C., which had disproportionately more plots because al Qaeda and affiliated movements, as well as other ideological terrorists, have identified them as targets.

The most-common motivations for ST-CP attacks have been personal (i.e., nonideological grievances), followed by terrorism and racial and ethnic extremism.

Figure S.1 shows that the ST-CP locations targeted have been diverse and often directly accessible.[2] Education and private buildings (workplaces) are the most–frequently targeted types of ST-CPs. In general, locations in which a would-be attacker (most commonly, an active shooter) had ready access to a dense crowd on scene had the highest average level of lethality (close to six deaths, on average, compared with fewer than three when there was not a dense crowd present). Not surprisingly, locations that typically have large crowds without controlled entries, such as houses of worship, shopping malls, restaurants, bars, and nightclubs, had the highest average lethality.

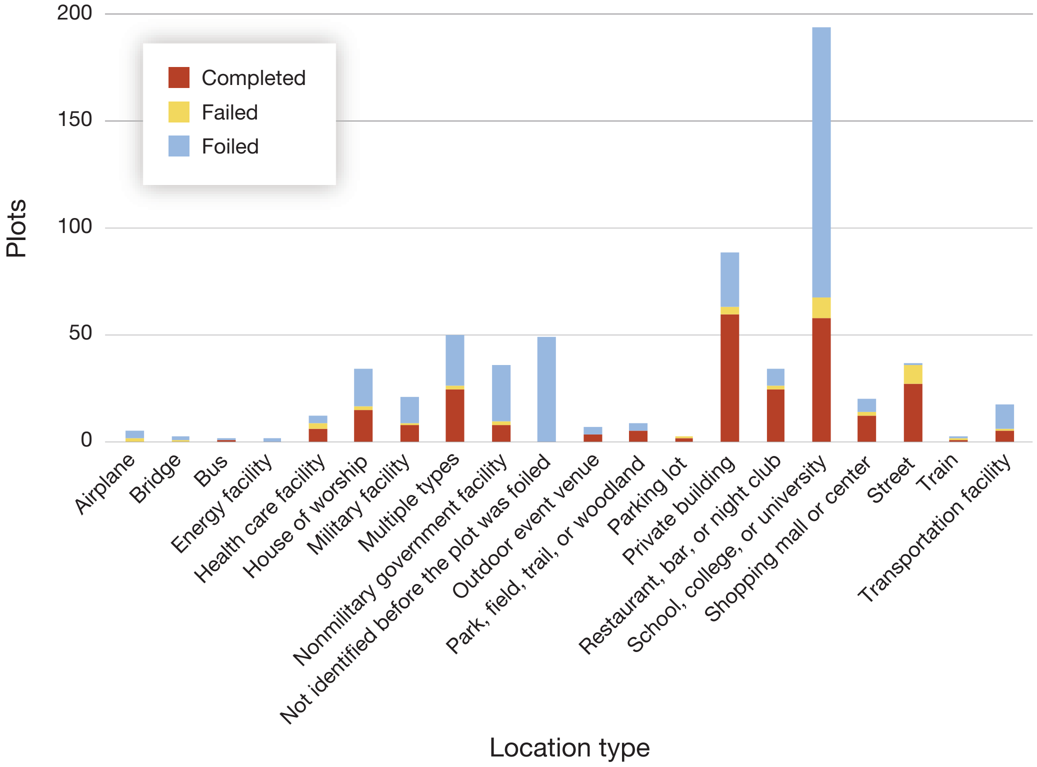
Security Measures and Spending for Soft Targets and Crowded Places

We found that security spending was growing but to an uncertain effect. Data on spending show significant growth after the shooting at Sandy Hook Elementary School in Newtown,

[1] Results reported in this section are based on an analysis of data on ST-CP attack plots from Hollywood et al., *Mass Attacks Defense Toolkit*.

[2] *Directly accessible* is defined as having no physical security measures impeding access.

FIGURE S.1
Mass-Attack Plots, by Location Type



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated all cases (*n* = 628).

Connecticut, in 2012: Spending on security systems has risen 52 percent since 2012, while the total increase in spending on guards and patrols was 15 percent between 2013 and 2020. In 2020, total spending reached $56.2 billion, with $30.2 billion in guard and patrol services and $26 billion in security services.

As part of this project, we developed a prototype costing model for school security. Initial results provide a range-of-magnitude estimate for annual security costs for U.S. schools in the billions of dollars, with nonlabor costs estimated at $1.5 billion to $10.0 billion annually and labor costs approximately three to five times nonlabor costs. The preceding estimates for all U.S. security spending—$56.2 billion—does provide an upper bound on school security costs. As discussed in the body of the report, the range reflects substantial uncertainties about the costs required to secure schools under a variety of conditions.

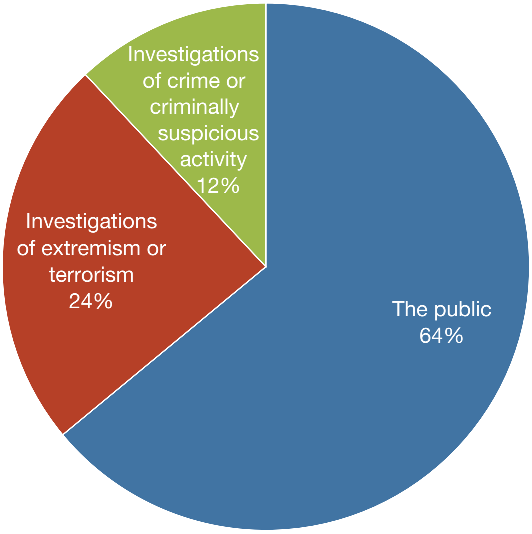
We identified a large amount of literature on security measures. However, we found few articles directly assessing the effectiveness of those measures; the rarity of mass attacks makes direct evaluations of whether security measures reduce attacks and casualties generally infeasible. Among potential security measures, we did locate articles in the literature indicating that security managers and access control measures specifically were cost-effective.

Prevention measures are perhaps the most important because they can and have halted many plots before they reached execution. Reports of warning signs have been key. As shown in Figure S.2, almost two-thirds of warnings about attack plots have been tips from the public, with other warnings coming from ongoing investigations of extremism and terrorism, as well as investigations of criminal and suspicious activity that appeared unrelated to an attack plot. When warning signs of a plot were reported to authorities in advance of an attack, the plot was foiled more than 80 percent of the time.

A Layered Approach to Improving Security for Soft Targets and Crowded Places

A system-based, or layered, approach helps security measures work together to improve the chances that an attack will be stopped or mitigated, guarding against single points of failure. Figure S.3 shows an example ST-CP attack chain—steps that a perpetrator must complete to kill a large number of people—and corresponding defensive layers that can foil or at least mitigate the attack at any point.

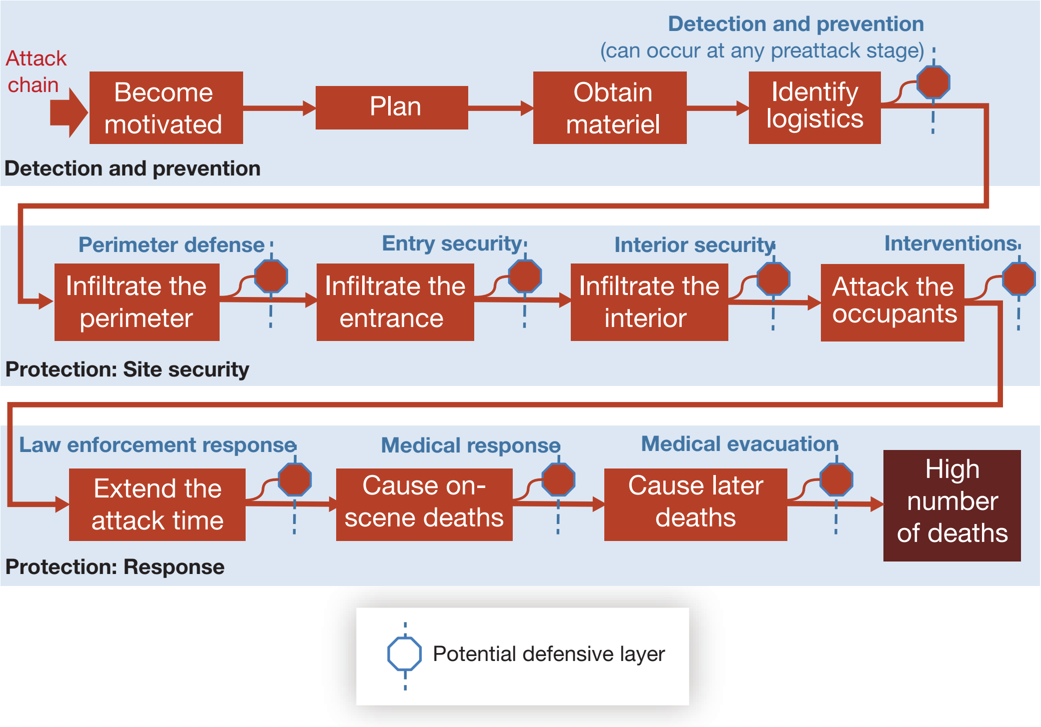
FIGURE S.2
Sources of Warning Signs About Attack Plots



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated all foiled cases in the dataset (*n* = 326).

FIGURE S.3
The Attack Chain and Corresponding Defensive Layers for Soft Targets and Crowded Places



In the rest of this section, we describe the requirements for investments are intended to help bolster one or more of these defensive layers.

Nonmateriel Investment Priorities

In the short term, the highest-priority nonmateriel investments are as follows:

- Improve public education about what warning signs to report and how (including warning signs that someone is suspiciously seeking weapons), as well as how to respond when in an attack. Response training should clarify the run/hide/fight protocol:
  - Run, if possible, to escape to safety, which can be a secure room in a facility, not just outside.
  - Hide, if running is not possible, in a location that is both out of view and locked away from the attacker.
  - Fight, if running and hiding are not possible. When facing an active shooter, groups should tackle the shooter from multiple directions, with the same aggressiveness with

which the public has been trained to stop people attempting to hijack an airplane, post–September 11, 2001.

- Provide funding and training for threat assessment (prevention) and protection management teams.
- Provide funding and training to improve response command, control, and communications.

Materiel Investment Priorities

The most-promising short-term investments are for core security equipment, including both new procurements and the maintenance of existing systems, ensuring the effectiveness of those systems. These include support for the following:

- access control systems, starting with door locks and strengthened windows that can keep attackers out of interior spaces containing crowds
- emergency exit equipment, including doors, one-way locks, and signage
- medical supplies for stopping bleeding and meeting Committee for Tactical Emergency Casualty Care treatment standards
- monitoring and alerting systems that allow people on scene (whether security personnel or not) to sound alarms that an attacker is present; these can include sensor systems that can detect weapons or weapon use at a distance, increasing time to respond
- communication systems that allow calling for an emergency response, coordinating with responders, and coordinating with people on scene on what to do.

Site Plan Priorities

Having entry areas that are securable and observable can prevent attackers from entry and provide early warning. An entry area should have at least two layers of lockable doors with secured spaces between them, so that, if an attacker gets through one doorway, they can still be denied entry to the larger building. Exit doors and accessible windows should be secured. Inside, having securable interior areas with locking doors can protect bystanders if an attacker gets into the building. Providing additional exits and signage to them can assist bystanders in evacuating.

Research and Development Priorities

For attack prevention, research, development, testing, and evaluation (RDT&E) priorities are as follows:

- Provide for ongoing tracking and analysis of ST-CP attacks and attack attempts.
- Improve capabilities for deterrence and dissuasion, steering would-be attackers away from pursuing their attacks.

- Develop indicators for suspicious seeking of weapons and ammunition, then develop and deploy corresponding education programs for both federally licensed dealers and the public.
- Develop protocols for the wellness checks that officers and other in-field service providers use to initially assess a person reported as being at high risk.

For ST-CP protection, including on-site security measures and attack response, RDT&E priorities are as follows:

- Develop a model concept of operations for protection of open spaces, given that many traditional security measures (notably, secured entry points) will not be present.
- Develop improved concepts for response command, control, and communications.
- Conduct more evaluations on the effectiveness and efficiency of security measures. We have learned of increasing development of systems incorporating artificial intelligence, so we anticipate that more evaluations of such systems will be needed.

Contents

Figures and Tables

Figures

Tables

CHAPTER 1

Introduction and Methodology

This report covers a comprehensive landscape assessment of the threat to soft targets (STs) and crowded places (CPs) (ST-CPs) and corresponding security measures. This analysis integrates literature reviews, analysis of data on attack plots, grant data reviews, and security modeling to identify needs for improving security and recommended research and investment priorities for addressing those needs.

Background

U.S. Department of Homeland Security Definitions of Soft Targets and Crowded Places

In 2018, the U.S. Department of Homeland Security (DHS) released its "Soft Target and Crowded Places Security Plan Overview" to provide key stakeholders in the public and private sectors an overview of its mission to enhance security and resilience of ST-CPs. The plan defines ST-CPs as follows:

> Soft Targets and Crowded Places (ST-CPs), such as sports venues, shopping venues, schools, and transportation systems, are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack.[1]

In recent years, attacks on ST-CPs have predominantly been active shootings. Other types of attacks have been present, including vehicle rammings of crowds, mass stabbings, and explosives.

The plan identified multiple roles for DHS to assist in securing the country's ST-CPs, including security operations and support; providing awareness, intelligence, and information-sharing; supporting partner capability and capacity-building; and carrying out research and

[1] DHS, "Soft Target and Crowded Places Security Plan Overview," p. iii.

development (R&D) to improve capabilities. The plan also emphasizes the importance of scalability and efficiency in bolstering ST-CP security:

> **Need for ST-CP Security to be Affordable and Scalable.** The ST-CP landscape includes hundreds of thousands of venues and services millions of people daily. Thus, to truly enhance ST-CP security and preparedness, the Department must find ways to expand the scale and reach of its programs, such as through partnership and empowerment approaches and cost-sharing. Additionally, in recognition that the resources available to dedicate to security are limited across the spectrum of ST-CP partners, the Department must work to make security technologies, tools, and resources as affordable as possible.[2]

Similarly, objective 4.2 of DHS's *Strategic Framework for Countering Terrorism and Targeted Violence*, issued in September 2019, identified ST-CPs as urgent focus areas and identified several priority action areas, including the following:

- enhancing security of STs
- enabling nationwide cybersecurity and infrastructure security
- upgrading biodetection methodology
- integrating frontline operator capabilities with DHS response and recovery efforts in the event of an attack using a weapon of mass destruction.[3]

The Importance of Threat and Defense Analysis for Soft Targets and Crowded Places

ST-CP attacks are rare for a country of more than 330 million people, but they still result in significant loss of life. For example, just one type of attack on ST-CPs—active shootings—were responsible for 100 killed in 50 attacks in 2022 and for 103 killed in 61 attacks in 2021.[4]

Furthermore, one of the most-striking features of the ST-CP threat is the extreme and widespread level of fear it generates throughout American society. As just a few examples, in 2019, almost half of U.S. respondents reported to Gallup that they feared being the victim of a mass shooting.[5] Another 2019 poll showed that one-third of U.S. adults were so afraid of mass shootings that they avoided certain places and events.[6] Within schools, specifically, a 2018 survey revealed that more than half of teens, as well as more than half of parents, said

[2] DHS, "Soft Target and Crowded Places Security Plan Overview," p. 14.

[3] DHS, *Strategic Framework for Countering Terrorism and Targeted Violence.*

[4] Federal Bureau of Investigation (FBI) and Advanced Law Enforcement Rapid Response Training Center at Texas State University (ALERT), *Active Shooter Incidents in the United States in 2022*, p. ii; FBI and ALERT, *Active Shooter Incidents in the United States in 2021*, p. 4.

[5] Brenan, "Nearly Half in U.S. Fear Being the Victim of a Mass Shooting."

[6] Ducharme, "A Third of Americans Avoid Certain Places Because They Fear Mass Shootings."

they were at least somewhat worried about a mass shooting happening at their school.[7] More broadly, four in ten Americans in a 2022 poll said that they felt that it was likely they would be a victim of gun violence sometime in the next five years.[8] The American Psychological Association has issued a warning that the "regularity of mass shootings is razing Americans' mental health."[9] ST-CP attack prevalence has even been used in anti–United States propaganda.[10]

The high costs, both direct loss of life and indirect loss of mental health and welfare of people in the United States, make reducing the threat of ST-CP attacks a high priority. At the same time, as noted in the security plan, measures introduced to reduce ST-CP attack risks must be scalable and efficient.[11] There is also a call to avoid backfiring effects of security measures; for example, authors of a 2021 article found that active-shooter drills in schools increased social media indicators of anxiety, stress, and depression by about 40 percent.[12]

Overview of the Methodology

In response to these challenges, DHS's Science and Technology Directorate chartered the Homeland Security Operational Analysis Center (HSOAC) to carry out a landscape assessment of the ST-CP threat, major vulnerabilities, status of existing security measures and initiatives, and ways to improve the allocation of ST-CP security resources.

Research Questions

This research is intended to answer the primary research question: *How can prevention, protection, and response and recovery investments reduce the risk of casualties from attacks on ST-CPs?*[13]

Subsidiary research questions include the following:

- How has spending on ST-CP security changed in the past 30 years?
- How have incidents changed over that time (in, for instance, frequency or lethality)?

[7] Graf, "A Majority of U.S. Teens Fear a Shooting Could Happen at Their School."

[8] Doherty, "Poll."

[9] Abrams, "Stress of Mass Shootings Causing Cascade of Collective Traumas."

[10] For example, Ministry of Foreign Affairs of the People's Republic of China, "Gun Violence in the United States."

[11] DHS, "Soft Target and Crowded Places Security Plan Overview."

[12] ElSherief et al., "Impacts of School Shooter Drills on the Psychological Well-Being of American K–12 School Communities."

[13] Direct costs include casualties, property damage, and emergency services. Indirect costs include spending on response and impact on community and businesses.

- How have threat actors and target types changed in the past ten years?
- What factors affect either the number of incidents *or* the lethality of incidents?
- What opportunities (in, for instance, programs, policies, or technology) are there for reducing the number or lethality of incidents?
- What are the unintended (positive and negative) consequences of increased ST-CP security?
- How are ST-CP priorities aligned with factors affecting the frequency and lethality of incidents? Are there any significant gaps or shortfalls?

Technical Approach

To address these questions, we carried out the following tasks, with details provided in the rest of this section.

Understanding the Threat to Soft Targets and Crowded Places

We characterized the nature of the ST-CP threat today through an analysis of peer-reviewed and gray literature.

We reviewed existing databases that include both ST-CP incidents and foiled plots to attack ST-CPs. The principal database employed is the Mass Attacks Defense Toolkit (MADT) dataset, which contains more than 600 cases of both prevented and executed attack plots on the public, almost all of which occurred at ST-CPs.[14]

The MADT defines *mass attack* or *mass-attack plot* as

> any violent attack or plot (conspiracy) to engage in an attack in a public space (including schools and workplaces) in the United States that endangered, or was intended to endanger, the lives of four or more people. In this definition, we exclude attacks specifically related to gangs, organized crime violence, terrorism plots prior to 2002 (to avoid statistical and operational complications from including the September 11, 2001 and Oklahoma City attacks), and domestic violence incidents in which the unaffiliated public is not deliberately targeted.[15]

The MADT organizes attack plots into three major categories:

- **foiled:** attacks that were found and prevented before initiation
- **failed:** attacks that were initiated but failed to penetrate the target; an attack of this type can still produce casualties if a perpetrator begins an attack but is stopped or arrested before entering the venue
- **completed:** attacks that gained access to the target.

[14] Hollywood et al., *Mass Attacks Defense Toolkit*.

[15] Hollywood et al., "About the Mass Attacks Defense Toolkit."

We also identified six historical case studies for comparative analysis, to draw deeper lessons learned. These were selected to be exemplars of both low- and high-casualty attacks, across multiple types of attacks (shootings, explosives, and vehicle rammings), at multiple kinds of sites, and with extensive lessons-learned material.

In addition, we held discussions with internal and external risk analysis experts to obtain their perspectives on trends in attack plots and security measures. We combined these analytic findings to characterize the major approaches used to target, create, and execute ST-CP attacks, described in Chapter 2.

Assessing Vulnerabilities and Current and Planned Solutions

We coordinated with the Science and Technology Directorate to identify experts within key agencies in DHS, other parts of the U.S. government, and industry who are engaged in ST-CP security. Through a series of interviews, we received these experts' perspectives on major ST-CP vulnerabilities, existing or planned solutions, and areas that required additional intervention. In this assessment, we also examined ST-CP expenditure data, by target type, security solution applied, and source of funds (federal, state, local, tribal, or territorial [SLTT]), to the extent possible, given data limitations.

Assessment of Preparedness and Response and Recovery Spending

We reviewed and assessed existing data, models, and analyses related to recent ST-CP attacks and security investments to prevent attacks. We compared the relative benefit of each type of investment for reducing the frequency and lethality of attacks. Where possible, we assessed the expenditure over time of the entire security enterprise and identified related changes in the frequency and lethality of ST-CP attacks. We analyzed aggregate and individual case data, where available, and performed a historical comparative analysis of six ST-CP attacks.

Landscape Assessment

In the landscape assessment, we assembled the results of all the prior tasks to provide an overall characterization of the nature of the ST-CP threat, vulnerabilities, and ranges of likely consequences, resulting from the various types of ST-CP attacks in the United States. The landscape assessment included a list of potential research and programmatic solutions, developed through a combination of open literature review, market analysis, and review of recent awards and grants, that could reduce the vulnerabilities.

Research and Implementation Road Map

The conclusion of this report—the road map—uses the results of the landscape to derive actionable recommendations to harden ST-CP security and improve ST-CP investments to (1) develop measurement techniques and data collection processes that will facilitate the evaluation of solutions and (2) help advance RDT&E efforts to improve ST-CP security.

Overall, this project is intended to help identify effective and efficient pathways through which the risks of ST-CP attacks, and casualties during those attacks, can be diminished.

Prior Work on Which This Project Builds

This project builds on prior HSOAC research projects. Jackson, Rhoades, and their colleagues provided findings on existing approaches to prevent mass attacks (specifically, ideologically motivated attacks) and recommendations to strengthen these approaches.[16] Zycher provided a general benefit–cost framework that informed the cost analyses described later in this report.[17]

Moore and her colleagues, as well as Steiner and her colleagues, provided frameworks for security at kindergarten through grade 12 (K–12) schools, including diagrams of the layout and interaction of security systems.[18] Although these are for K–12 contexts, most of the framework elements are broadly applicable to ST-CPs. These framework elements and diagrams informed the development and diagramming of the ST-CP security layers presented in this report.

As mentioned, this project leverages the MADT dataset of more than 600 mass-attack plots, almost all of which were against ST-CPs.[19] This project also leverages the MADT's findings, especially those on prevention, because the toolkit included a deep analysis of the warning signs, threat assessment processes, and diversion and investigative steps needed to stop attacks. This report refers to these findings in its coverage of prevention measures to provide additional details.

Finally, this project builds on HSOAC's support to the U.S. Secret Service's (USSS's) "Mass Attacks in Public Spaces" project, leveraging the findings and cases in that project's reports.[20]

Methodological Details

A Quantitative Analysis of Prior Cases Involving Soft Targets and Crowded Places

The MADT includes data on mass attacks, attempted mass attacks resulting in few casualties, and mass-attack plots that were prevented in advance. *Mass attack* has been defined as "any violent attack or plot (conspiracy) to engage in an attack in a public space (including schools and workplaces) in the United States that endangered, or was intended to endanger, the lives

[16] Jackson, Rhoades, et al., *Practical Terrorism Prevention*.

[17] Zycher, *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*.

[18] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Steiner et al., *Challenges in Implementing Physical Security Measures in K–12 Schools*.

[19] Hollywood et al., *Mass Attacks Defense Toolkit*.

[20] National Threat Assessment Center (NTAC), *Mass Attacks in Public Spaces*.

of four or more people."[21] The dataset provides data on cases from 1995 through 2020, with the following exclusions:

- attacks related to criminal violence and domestic violence in which the unaffiliated public was not deliberately targeted
- terrorism cases prior to 2002, to avoid statistical and operational complications from the September 11, 2001 (9/11), and Oklahoma City attacks.

The toolkit data drew on 27 prior datasets to identify cases, plus custom internet searches to find additional cases from 2016 through 2020 to help characterize more-recent trends.[22] To further ensure that our searches captured events that occurred in 2020, we also consulted the Gun Violence Archive and consulted FBI press releases for that year.[23]

The dataset contains information on 628 cases. Although the original MADT dataset focused on a subset of the available variables (17 subject variables, four attack variables, nine event variables, and three response variables), this analysis incorporated additional existing variables not used in the MADT and new variables coded after the release of the MADT.[24] Specifically, we reviewed existing cases to add information on incident site configuration, incident site types, attributes associated with low-fatality incidents, and elements of subject (aggressor) location during an incident, including level, distance, and movement. Additionally, information on subject motives were updated for consistency with revised DHS terminology.

After case review and data processing, we used a series of analytic methods (primarily using the statistical software R and Microsoft Excel) to create numerical and graphical summaries of key variables and relationships.

A Literature Review on Guidance and Protective Measures

To identify top findings on protective factors for ST-CPs, we conducted internet searches to capture past and current federal, state, and local government and nongovernmental guidance, regulations, and recommendations related to ST physical security. We also conducted searches of the research literature—peer-reviewed and non–peer-reviewed publications—focused on the use of technology and physical security measures to keep various categories

[21] Hollywood et al., "About the Mass Attacks Defense Toolkit."

[22] Hollywood et al., "About the Mass Attacks Defense Toolkit," provides a full list of mass-shooting datasets and their citations. The search strings contained the following terms: "'at random' attack," "foiled attack," "prevented mass shooting," "mass attack prevented," "bombing prevented," "bombing plot," "mass attack," and "shooting plot."

[23] For 2020 specifically, to maximize the number of plots we could find from that year, we added the following search strings: "knife attack," "car attack," and "truck attack."

[24] For more information about the dataset and how the data were collected and processed, see Hollywood et al., "About the Mass Attacks Defense Toolkit."

of STs safe. We performed searches using Google (for government guidance and regulations and other nonacademic references) and Google Scholar (for academic references). We also reviewed references listed in sources we identified as highly relevant. Our search string was as follows:

> "soft target" OR "crowded place" OR "stadium" OR "school" OR "school building" OR "school facility" OR "house of worship" OR "transportation" OR "mass transit" OR "healthcare" OR "hospital" AND "physical security" OR "security" OR "design security" OR "safety" OR "design safety"

Based on additional trends observed in the past two years, especially since summer 2020, and to identify additional sources addressing mass attacks in the context of mass protests or demonstrations, we added the following search string to our Google search:

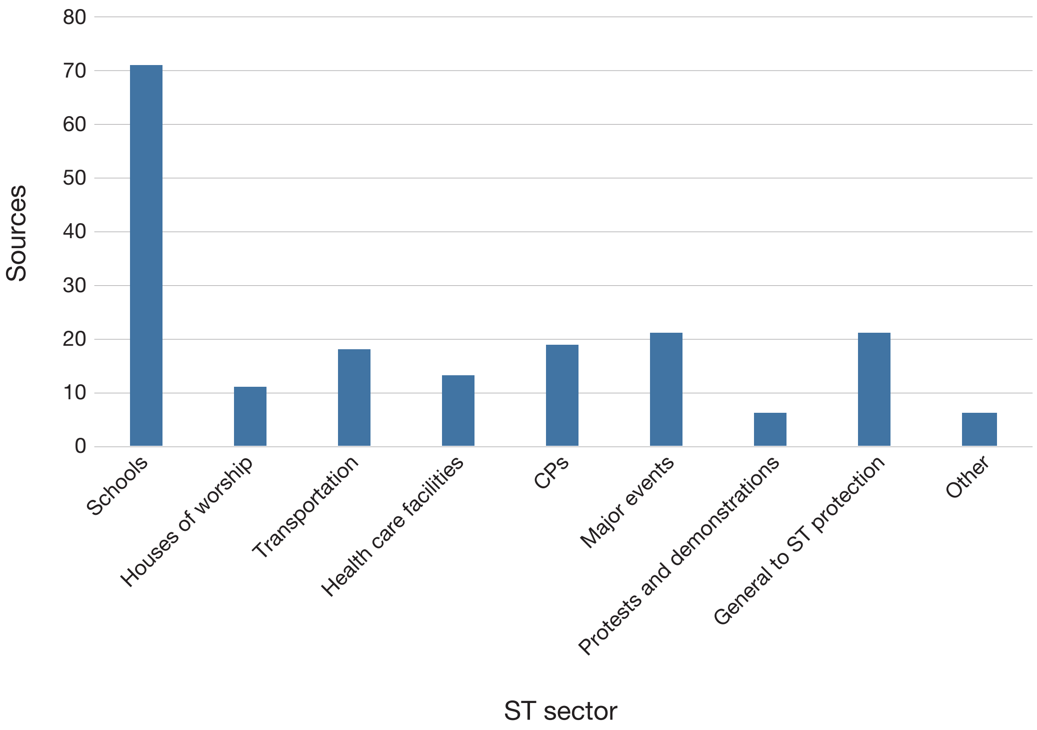
> "vehicular ramming" AND "protest" OR "demonstration"

We restricted our search to documents published or produced between 2002 and 2022. Our search netted 178 results focused on the use of technology, physical security measures, and policies to enhance security across different ST sectors. We also collected 22 after-action reports (AARs) of mass attacks in public spaces between 2007 and 2022, which focused primarily on responses to mass attacks (as opposed to protective measures in place at a facility or specific space prior to an attack). Seven reviews were conducted by the National Policing Institute, and six were conducted by local or state law enforcement (LE) or emergency management agencies that took part in the response to these incidents. Three were authored by commissions or committees established in the aftermath of specific incidents to identify points of failure in protection, mitigation, and response, as well as strategies for improvement. Federal agencies published reports about the responses to two incidents (one occurring at a federal facility), and the remainder were conducted by private-sector analysts.

We reviewed each document (including each AAR) for its relevance to our topic and coded each one as highly relevant (1), moderately relevant (2), or likely not relevant (3). One hundred nineteen sources (including 16 AARs) were coded as highly or moderately relevant, and we included these in our analyses. Figure 1.1 shows the number of highly or moderately relevant sources addressing specific ST sector types as identified in our review.

Most of the relevant sources that we identified in our review consisted of federal-level guidance or peer-reviewed studies about protective measures. Figure 1.2 provides an overview of our sources, by category. Additional source categories (not pictured in Figure 1.2) included case studies (eight sources), opinion pieces (eight sources), and issue and policy briefs (five sources).

FIGURE 1.1
Number of Relevant Sources, by Soft-Target Sector



SOURCE: Features data from our analysis of the 178 sources identified in the literature review.

Subject-Matter Expert Interviews

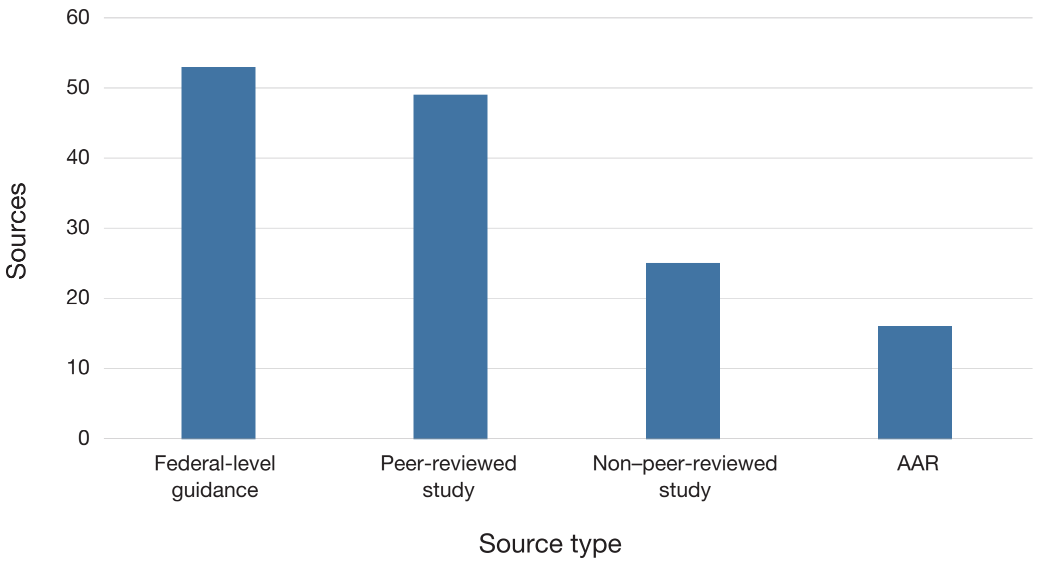
Semistructured subject-matter expert (SME) interviews were conducted to gain insights into the current state of the ST-CP security environments, security practices, emerging technologies, and cost trends. The interview candidates were chosen from a diverse background of security specialists. These included regional LE personnel and intelligence specialists, security industry system integrators, cost experts, and technology vendors and security industry association leaders.

The questions asked during the interviews mirrored the research questions previously mentioned. Additional topics discussed included

- trends in technology, including the growth of artificial intelligence (AI) in ST-CP security planning
- improvements and challenges in attack interdiction, coordination, and response
- trade-offs of technology and physical prevention methods' effectiveness, onsite security personnel, and cost.

FIGURE 1.2

An Overview of Major Source Types



SOURCE: Features data from our analysis of the 178 sources identified in the literature review.

The information gathered shaped the subsequent analysis of the current threat and trends in security practices and technology implementation, as well as the overall landscape assessment.

Case Study Analysis

To further understand the role that protective measures play in addressing mass attacks against ST-CPs, we also conducted case studies of six incidents between 2013 and 2021. The purpose of the case studies was to compare key aspects of each incident and evaluate areas that affected the number of fatalities. To do so, we selected cases that captured variation along eight key criteria:

- location of the incident (the ST sector)
- weapon used in the attack
- number of fatalities
- bystander responses during the attack
- protective measures in place before and during the attack
- site configuration
- crowd density
- attacker movement and distance from targeted individuals.

Five of our six case studies were selected from the sample of completed mass-attack incidents included in the MADT. The sixth, the Manchester Arena bombing in the United Kingdom, was chosen because it provided information on a significant bombing event. Table 1.1 provides an overview of our selected cases and variation along three of the key variables. We discuss the results of our analysis in Chapter 3.

Grant Analysis

We conducted a review of available federal government–sponsored grants to better understand what investment opportunities were available for SLTT governments and other organizations to provide solutions to protect ST-CPs. We reviewed publicly available information on grants at the federal level (from, for example, U.S. Department of Health and Human Services, grants.gov; and Grants Office, homepage) supplemented by a more targeted review of announcements by departments and agencies.

We intended to provide a better understanding of how organizations spend grant awards. We reviewed press releases from various state homeland security agencies as part of that attempt to discover any announcements about how federal or state money was allocated. We hoped to illustrate trends or gain insights that could help improve federal spending aimed at protecting or hardening ST-CPs. Information on how grant money is spent on the specifics of ST-CP defense, however, is not available in a way that allows regular review by outside parties.

Our reviews were also supplemented by our SME interviews. Our findings, including brief characterizations of the most-relevant federal grant programs, are presented in Chap-

TABLE 1.1
Case Study Incidents and Key Variables

Incident	Year	ST Category	Total Fatalities	Weapon Used
Arapahoe High School shooting	2013	School, college, or university	1	Shotgun
Pulse nightclub shooting	2016	Restaurant, bar, or nightclub	49	Handgun; rifle
Manchester Arena bombing	2017	Stadium[a]	22	Explosives
MSDHS shooting	2018	School, college, or university	17	Rifle
El Paso Walmart shooting	2019	Shopping mall or center	22	Rifle
Waukesha Christmas parade ramming	2021	Outdoor event venue	6	Vehicle

SOURCE: Features information from Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: MSDHS = Marjory Stoneman Douglas High School.

[a] This is the one example we have of a plot targeting a stadium or arena. It is not in the MADT because it did not occur in the United States.

ter 4. We conclude with recommendations, including concurring with a U.S. Government Accountability Office report suggesting that DHS develop a mechanism that would allow spending to be reported and readily tracked.

A Review of Costs and Spending

Costs of security at schools can be estimated using information revealed by aggregate economic data and cost modeling of the elements included in a school security program. Each approach provides a distinct perspective of the costs of security at schools and carries associated limitations.

Cost estimates derived from aggregate economic data are top-down estimates based on reliable data collected at the national level annually. However, as described in this section, the datasets that include school security also include spending on security that is in addition to active-shooter security measures. Examples included in these data are security costs at facilities other than schools and costs included at schools for other reasons (e.g., preventing vandalism or theft). As a result, these cost estimates provide an upper bound on what security spending could be.

Costs derived from modeling the elements included in a school security program provide a bottom-up perspective of what the costs might be at a typical school and the implications of adoption of each element across schools for the spending on school security at the national level. The challenge of this approach is that elements of school security vary widely across schools, based on such factors as the size of the building and student body, layout, facility age, and approach used to integrate security into the education setting at both the school and district levels. Although these dimensions can be modeled using standards, guidelines, and data on school practices, doing so incorporates many assumptions into modeling and introduces substantial uncertainty into results. The methods described in the next section provide a range of estimates to account for these uncertainties.

Together, these two approaches provide information that helps one understand the nature and order of magnitude of spending on school security nationally, with a goal of understanding the costs within a factor of ±2 to ±5 times the cost estimates generated. However, as discussed in the section of Chapter 4 on cost-modeling results, the estimates resulted in a range within an order of magnitude.

The remainder of this section describes the methods used to generate top-down and bottom-up cost estimates from each of these perspectives.

Estimating Costs Based on Aggregate Economic Data

The aggregate economic data used for our top-down estimate include information from the U.S. Bureau of Labor Statistics compiled by the Federal Reserve Bank of St. Louis.[25] We leveraged the North American Industry Classification System (NAICS), which provides conve-

[25] U.S. Census Bureau, "Investigation and Security Services."

nient classification of business establishments. To measure security spending at the national level, we focused our efforts on investigation and security services (NAICS 561600), which included two relevant subcategories: security guards and patrol services (NAICS 561612) and security-system services (except locksmiths) (NAICS 561621). As mentioned in the previous section, we acknowledge that this classification is broader than ST-CP security spending. This also is limited to private security spending and excludes public spending via national, state, and local LE or federal grants discussed in the previous section.

We then accessed the annual total revenue dating back to 1998 for NAICS 561612 and NAICS 561621 and adjusted for inflation by scaling each year proportionally to the gross domestic product implicit price deflator index.[26] Lastly, to identify the key trends in private spending, we normalized the inflation-scaled revenue to 1998 dollar amounts and compared it with the producer price index for all commodities, which represents revenue across all industry sectors.[27]

Estimating Costs Using Models of the Elements of School Security

The bottom-up cost model used to estimate school safety and security hardening measures for K–12 public schools was developed using publicly available data on K–12 schools (e.g., student enrollment), construction cost data available from RSMeans and other sources,[28] and safety and security standards and guidelines.

The first step in developing the cost model was determining what safety and security hardening strategies to include within the scope of the estimate. Moore and her colleagues developed a system approach to physical security at K–12 schools based on review of literature on school security.[29] We used this approach, along with standards and guidelines produced by ASIS International, to develop a framework for developing the cost model.[30] Figure 1.3 provides an overview of the security components reflected in the framework.

The safety and security hardening measures include a combination of building upgrades (e.g., installing newer door locks, installing metal detectors, security cameras), site improvements (e.g., site lighting), and services (e.g., security patrol, school administration training). Table 1.2 lists the items included within the cost model, organized by cost category.

Once we established the scope of work, the next step in the development of the cost model was assigning unit costs for each of the security and safety hardening measures. The unit costs were derived primarily from RSMeans and academic literature. The unit costs from RSMeans, which account for both labor and material costs, are based on 2022 national aver-

[26] U.S. Bureau of Economic Analysis, "Gross Domestic Product."

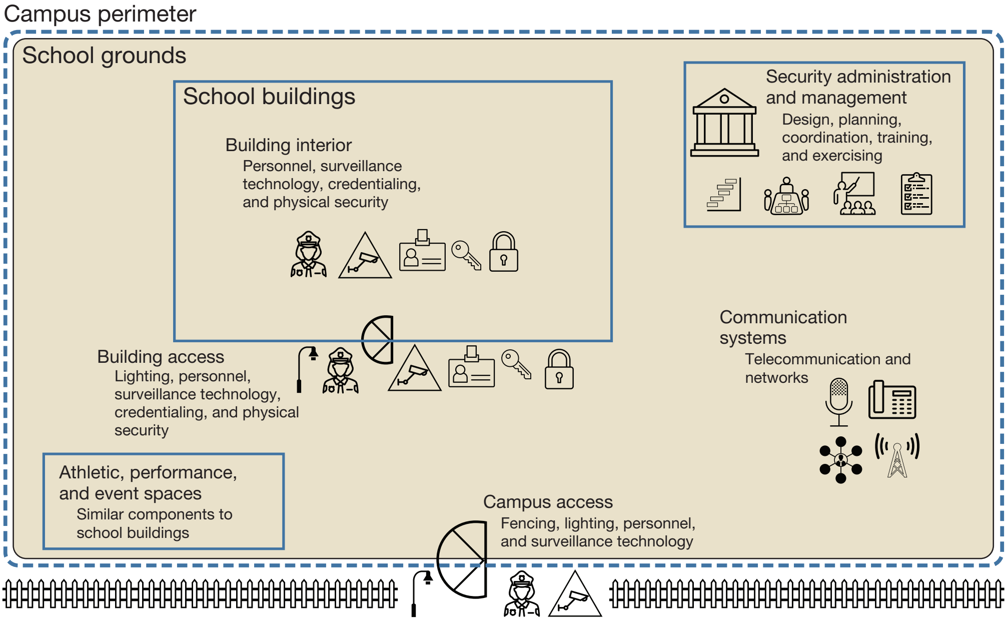
[27] U.S. Bureau of Labor Statistics, "Producer Price Index by Commodity."

[28] RSMeans is construction cost-estimating software and database. See RSMeans, homepage, for more information.

[29] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

[30] See ASIS International, *Physical Asset Protection*; ASIS International, *Protection of Assets*; and Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

FIGURE 1.3
Framework for K–12 School Security Represented in the Cost Model


Campus perimeter
School grounds
School buildings
Building interior
Personnel, surveillance technology, credentialing, and physical security
Security administration and management
Design, planning, coordination, training, and exercising
Communication systems
Telecommunication and networks
Building access
Lighting, personnel, surveillance technology, credentialing, and physical security
Athletic, performance, and event spaces
Similar components to school buildings
Campus access
Fencing, lighting, personnel, and surveillance technology

SOURCE: Features information in Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

age costs for repair and remodeling of a facility.[31] Unit costs for a given item can vary by model type, material, or other specifications. For example, costs for a classroom door can range from approximately $400 to $500, depending on whether the door is standard duty or heavy duty. To account for this uncertainty, the cost model includes a range of unit costs for each item (minimum, mean, and maximum).[32]

After we assigned the unit costs, the next step in the development of the cost model was determining the appropriate quantity to assume for each safety and security measure. To determine the appropriate quantity, we used a variety of resources and methods. First, we accounted for the variation in school size in terms of both the number of students enrolled and the square footage of the facility. Using a publicly available Homeland Infrastructure Foundation-Level Data dataset on K–12 public schools obtained from RSMeans and a 2016 overview of K–12 public school facilities in the United States,[33] we arrived at a range of school sizes using the following distribution points: minimum, 25th percentile, mean, median,

[31] Unit costs in RSMeans vary by the location selected (e.g., Los Angeles, San Francisco), year selected, and type of construction (e.g., new construction versus remodel or repair).

[32] For some unit costs, such as security patrol or security administration, a range was not available or applicable, so a single value was used instead.

[33] Filardo, *State of Our Schools*.

TABLE 1.2

Cost Categories for the Bottom-Up Cost Model

Cost Category	Item
Security personnel	Security guards
Surveillance technology	Security cameras and system
Metal detector	Walk-through metal detectors
	Security guards at metal detectors
Alarm and communication systems	Intruder-detection system
	Emergency PA system
	Emergency phone call stations
	Existing system integration
Physical security	Updated doors and locksets
	Site fencing and gates
	Security film on glazing
Credentialing system	Card access control system
Site improvements	Vehicle barriers
	Site lighting
Program design	Security and office administration
	Staff professional development and training
	SROs and programs

NOTE: PA = public address; SRO = school resource officer.

75th percentile, 95th percentile, and maximum. To estimate the quantity of certain building features, such as the number of classroom doors or square footage of windows, we used a parameterization method based on the gross square footage of the facility using the RSMeans Square Foot Estimator.[34] Quantities for certain items, such as the number of security cameras required, could not be calculated using the parameterization approach. For these items, we estimated the quantities using existing school floor plans as precedents.

Once we assigned a unit cost and quantity for each safety and security measure, we calculated the extended cost for each item and arrived at a total cost per school. From there, we annualized the cost using a 2.1-percent discount rate and a useful life for each asset. We scaled up the annualized cost per school by multiplying the costs by the total number of public schools in the United States. The final step in the development of the cost model was

[34] The RSMeans Square Foot Estimator is a feature available in RSMeans to estimate the total cost and quantity of building features (e.g., doors, windows) based on certain inputs, such as occupancy type, area, perimeter, and number of stories.

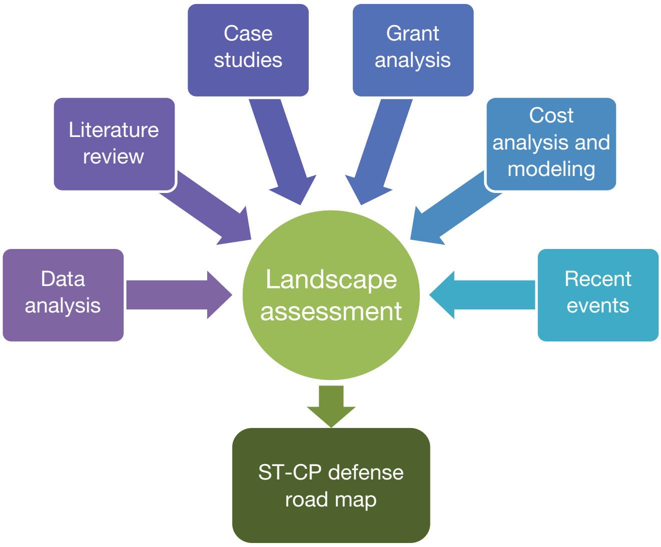
applying factors to account for schools that were implementing some of the safety and security strategies at that time. For example, researchers from the National Center for Education Statistics (NCES) found that approximately 91 percent of public schools in the United States between school year 2019 and school year 2020 used security cameras to monitor school grounds and facilities;[35] in the cost model, a 91-percent reduction was applied to the costs in the surveillance technology category to avoid overestimating the costs required for security cameras across the portfolio of schools in the United States. The cost model can be scaled to the district, state, and national levels based on assumptions and data about the number and characteristics of schools across the country.

Landscape Assessment

In the landscape assessment, we incorporated information from the data analysis, literature review, SME interviews, and cost analysis to form a summary picture of the current ST-CP security environment. Figure 1.4 illustrates this model.

The information fed into this model was used to create a layered visualization for defense against the ST-CP attack chain. As noted, this visualization of the attack chain is based on previous HSOAC research into system-based security methods for K–12 education facilities and adapted for the broader ST-CP threat environment.[36] The layered defense model consists

FIGURE 1.4
Landscape Assessment Structure



[35] NCES, *Safety and Security Practices at Public Schools.*

[36] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Steiner et al., *Challenges in Implementing Physical Security Measures in K–12 Schools.*

of three phases—prevention, site protection, and response—each of which identifies the key nodes in the attack chain at which security measures could foil attacks before execution, interdict them during execution, and respond to end an attack and minimize casualties. The landscape assessment then integrates the findings from the other analyses to identify issues—gaps, shortfalls, and needs for improvement—with current measures in the security layers.

The needs identified in the landscape assessment then inform the creation of a research road map that pinpoints specific candidate solutions to address the requirements. These include both research, development, testing, and evaluation (RDT&E) efforts and funding investments, along with relationships between them.

Organization of This Report

Chapter 2 of this report characterizes the threat posed to ST-CPs. The chapter includes an analysis of the evolution of the threat in the past 30 years, along with descriptions of plots by venue and geographic region, assailant motivations, and factors that affect the number and severity of casualties. Chapter 3 describes our assessment of preventive and protective measures, including common practices identified in the literature, results of quantitative analyses of past plots, and an analysis of six ST-CP attack case studies. Chapter 4 describes preparedness and response spending, including a description of security grants available for venue protection, a historical examination of security spending, and descriptions of preliminary security cost models. Chapter 5 presents our findings and a conceptual model of ST-CP attacks and security measures. Chapter 6 provides our recommendations and a road map for improving ST-CP attack prevention and protection. We provide our interview protocol in the appendix.

CHAPTER 2

Characterizing the Threat

The Evolution of Mass Attacks Against Soft Targets and Crowded Places

The threat to ST-CPs has evolved as U.S. society and culture have changed and technology has made it easy to post rationales, live stream events, and create the impression that the perpetrators of violent acts can become famous. The nature of the threat actor has also changed. Prior to 2016, al Qaeda, Daesh, and affiliated movement-related attacks were often responsible for large shares of attack plots; in the MADT data, these shares reached as high as 71 percent of plots in 2015 (and above 30 percent in 2013, 2011, and 2009). However, since 2017, these shares have not gone above 12 percent.

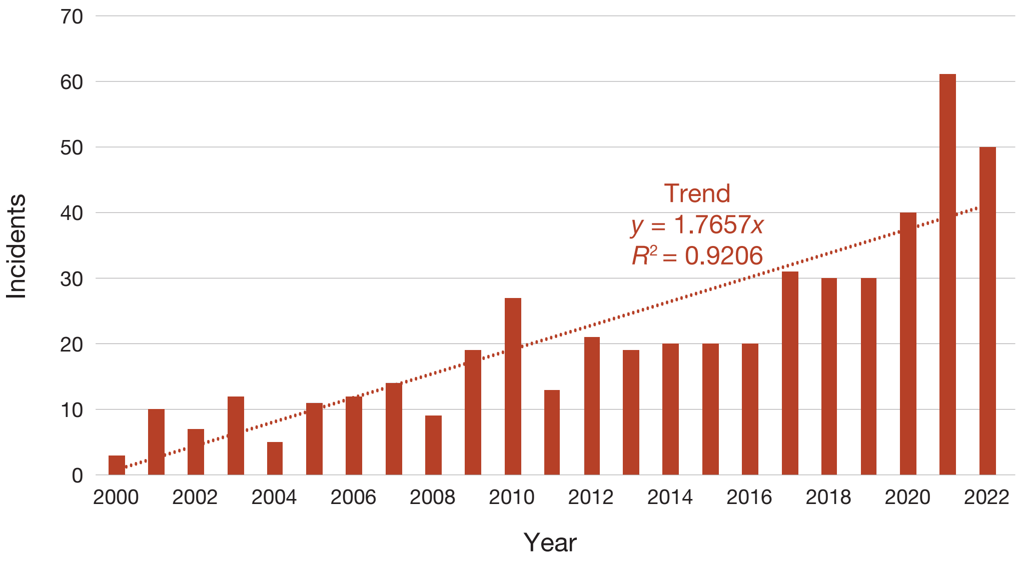
The number of active-shooter incidents has risen consistently since 2000. FBI data show these types of incidents from between zero and ten per year from 2000 to 2008, and the number increased to a high of approximately 60 incidents in 2021 before dropping to 50 in 2022. Figure 2.1 shows the trend over time.

Although it has generally not been observed as of this writing in late 2023, our interview data suggested a growing concern about the prospect of uncrewed aircraft systems (UASs) being used for attacks on ST-CPs. The use of UASs against ST-CP sites has become a concern in the ST-CP security sector. The unique characteristics of UASs could see their use grow in future years. UASs can carry explosive payloads and have the ability to maneuver into secure areas without detection. UASs can also give the operator the ability to act anonymously and a greater chance to avoid detection and capture. The growing use of UASs in both the private sector and government operations likely means that more people will have access to these systems in the future and the expertise to operate them, making the use of UASs for attacks increasingly likely.

The threat actor in ST-CP attacks has evolved over time from more–ideologically driven individuals and small groups (notably, with al Qaeda and Daesh motivations) to more individual attacks by perpetrators with personal grievances against specific groups or those with polygrievances. A polygrievance is multiple grievances that coalesce into a desire to act. The recent emergence of incels (men who have had difficulty connecting with women and thus

FIGURE 2.1

Active-Shooter Incidents in the United States Since 2000



SOURCES: Derived from FBI, *Active Shooter Incidents: 20-Year Review*; FBI and ALERT, *Active Shooter Incidents in the United States in 2020*; FBI and ALERT, *Active Shooter Incidents in the United States in 2021*; and FBI and ALERT, *Active Shooter Incidents in the United States in 2022*.

act on their frustrations by violently targeting women or groups associated with women) is a prime example.[1]

On the positive side, there have been few, if any, reported catastrophic terrorist plots on the scale of the 9/11 attacks or the Oklahoma City bombing, much less successful catastrophic attacks.[2] However, the evolution of the ST-CP threat includes more attacks that involved extensive surveillance of a target and risk assessments of an attacker's ability to cause the desired number of casualties. The growth and capabilities of information technology have also contributed to the changes in ST-CPs over the years. Now, extensive research and planning can be done online to identify potential targets and assess their security arrangements. This has been augmented by physical surveillance to determine target selection.[3]

In addition, online chat rooms, blogs, and the ability to live stream events have enabled potential attackers to connect with audiences globally in an effort to seek fame or spread their messages. The online world enables attackers to connect with like-minded people and post manifestos explaining their actions. Live streaming allows attackers to show their actions in real time, conveying a sense of importance that could be lacking in other parts of their lives.

[1] LE SME, interview with the authors, May 19, 2023.

[2] Inferred from data from Hollywood et al., *Mass Attacks Defense Toolkit*.

[3] LE SME, interview with the authors, April 3, 2023.

This can contribute to their believing that their actions will bring them fame and inspire others to take up their causes.[4]

One important note on the online aspect of ST-CP attacks is that it increases the opportunity to interdict an attack before it happens or to stop an attack in progress. It is currently desirable to shut down an attack's live stream to prevent it from reaching a wide audience. Some inside the ST-CP security enterprise raise the point that allowing live streaming to continue would allow LE responders to understand the tactical situation in real time and could help stop an attacker more quickly, possibly reducing casualties.[5] Insight into a possible attacker's mindset, through examining social media postings and identifying hostile content, can also help stop attacks before they happen. People close to a potential attacker with access to their social media accounts, the public, and social media companies can report suspicious or hostile behavior, raising red flags for LE to intervene.[6] As identified in Chapter 3, data from foiled attacks indicate that tips from the public, although not all online-related, make up the majority of reasons for foiled attacks.

Plots Against Soft Targets and Crowded Places, by Attack Venue and Geographic Region

Analysis of Target Types and Locations

Figure 2.2 shows the total number of mass-attack plots by attack location, using the cases in the MADT (covering 1995–2020). As shown, by far the greatest number of plots were against education facilities (schools, colleges, and universities). However, these plots were also some of the likeliest to be foiled in advance (largely thanks to tips, as discussed in Chapter 3).[7] Other locations with comparatively high numbers of plots included private buildings (workplaces), government facilities, houses of worship, open streets, and restaurants, bars, and nightclubs.

Comparison of Attacks on Soft Targets and Crowded Places, by Geographic Region

In general, ST-CP attacks showed little concentration by geographic region. Figure 2.3 shows the numbers of plots by Federal Emergency Management Agency (FEMA) region; as shown, overall numbers of plots largely correlate with the total populations in each region.

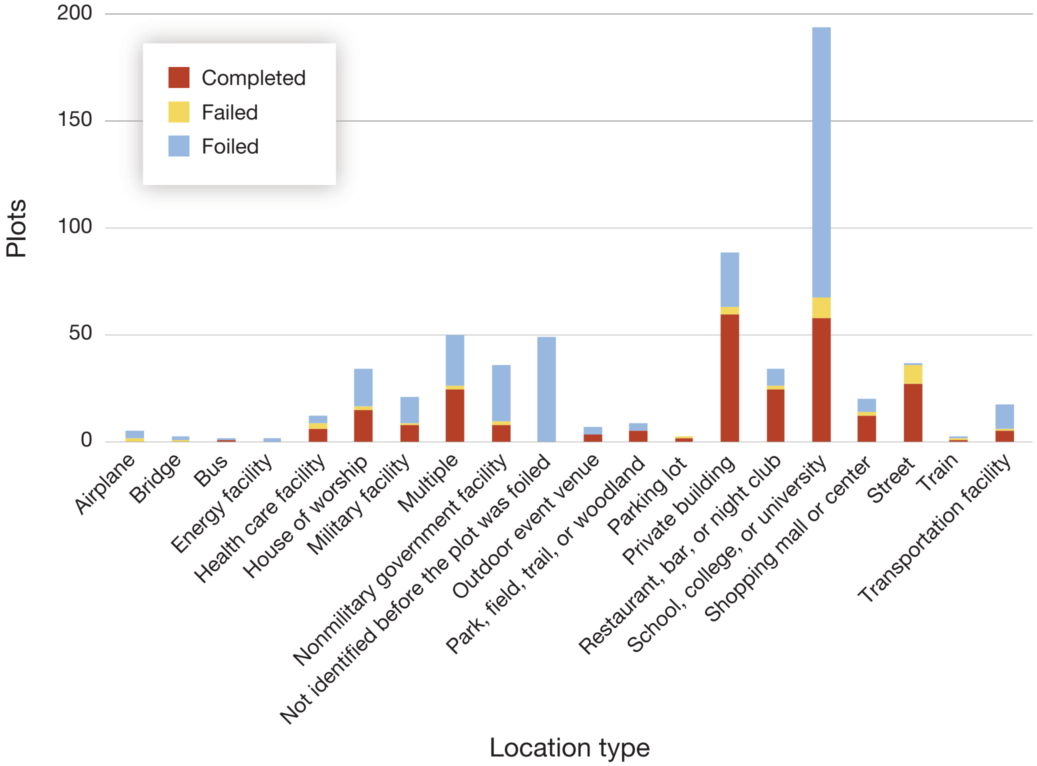
[4] LE SME, interview with the authors, May 19, 2023.

[5] LE SMEs, interview with the authors, May 19, 2023.

[6] LE SMEs, interview with the authors, May 19, 2023.

[7] The relative prevalence of school plots discovered through tips opens up the possibility that there are also sizable numbers of plots on other types of locations that collapsed on their own but went undetected.

FIGURE 2.2
Mass-Attack Plots, by Location Type



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated all cases (n = 628).

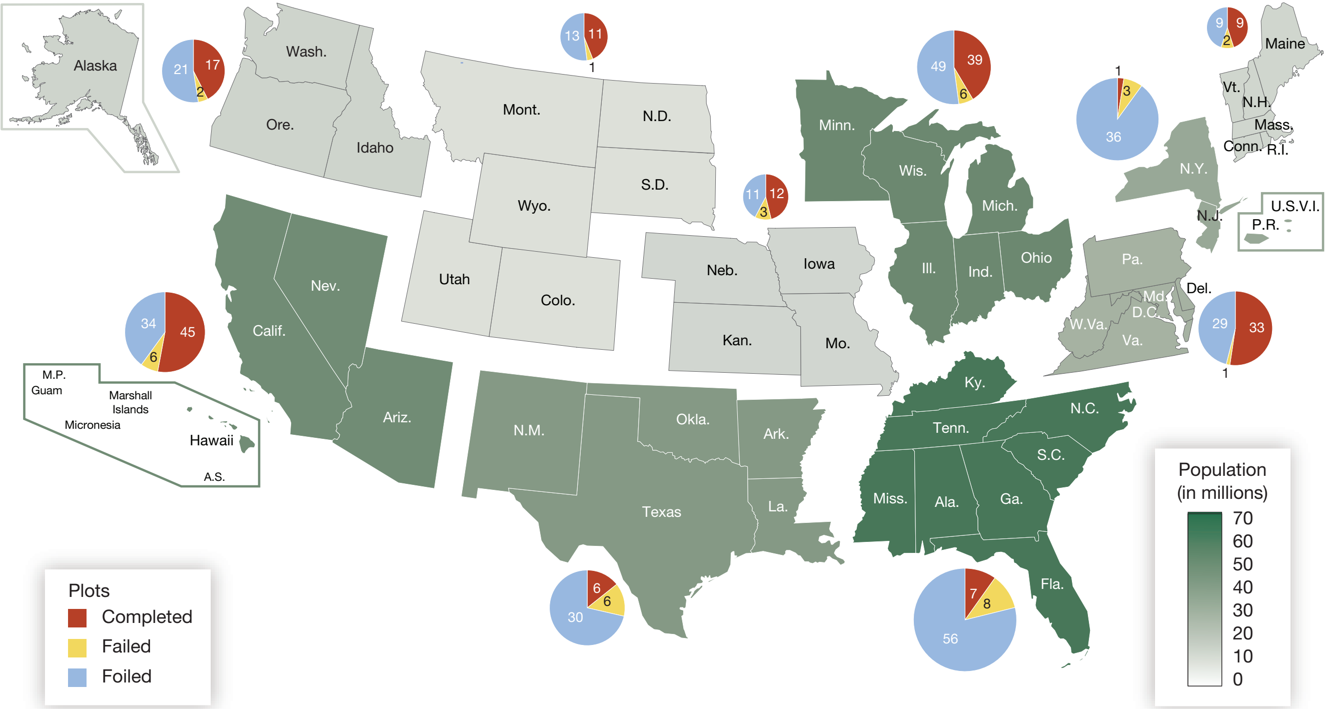
In general, proportions of plots by state also roughly matched state populations. The two exceptions were New York and the District of Columbia; both had disproportionately high numbers of plots, largely because of would-be terrorists' focus on New York City and Washington, D.C.

Mass-Attack Plots on Soft Targets and Crowded Places, by Weapon Type

Figure 2.4 shows the types of weapons used (actual or intended) in mass-attack plots. As shown, a majority of the plots were shooting attacks. Plots involving explosives were a distant second; also note that explosive plots were mostly stopped in advance. Knife and vehicle-ramming attacks also had presences.

FIGURE 2.3

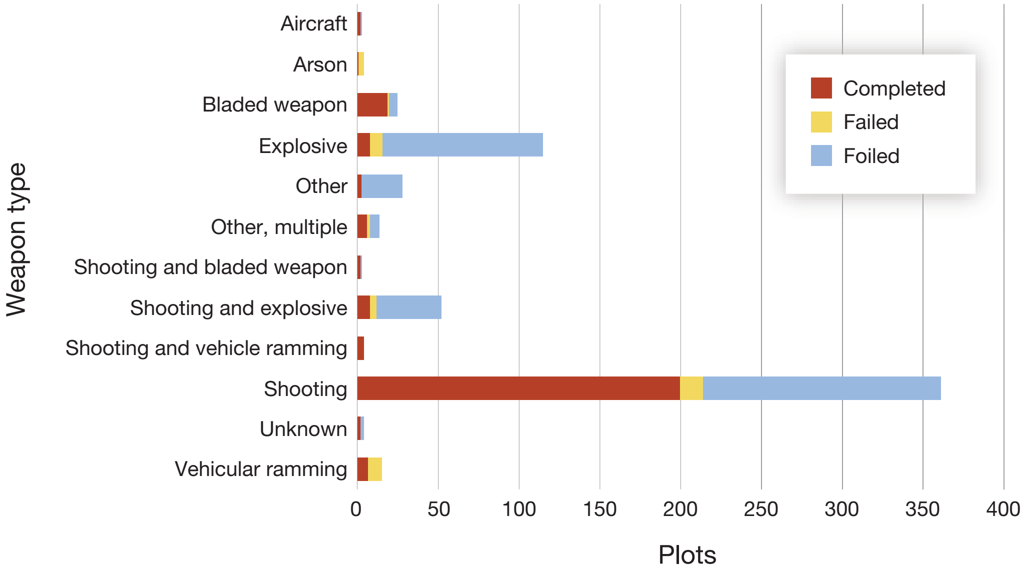
Attack Plots and Total Populations, by Federal Emergency Management Agency Region



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated any case in which the state was identifiable (*n* = 587).

FIGURE 2.4
Mass-Attack Plots, by Type of Weapon Used



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated all cases (*n* = 628).

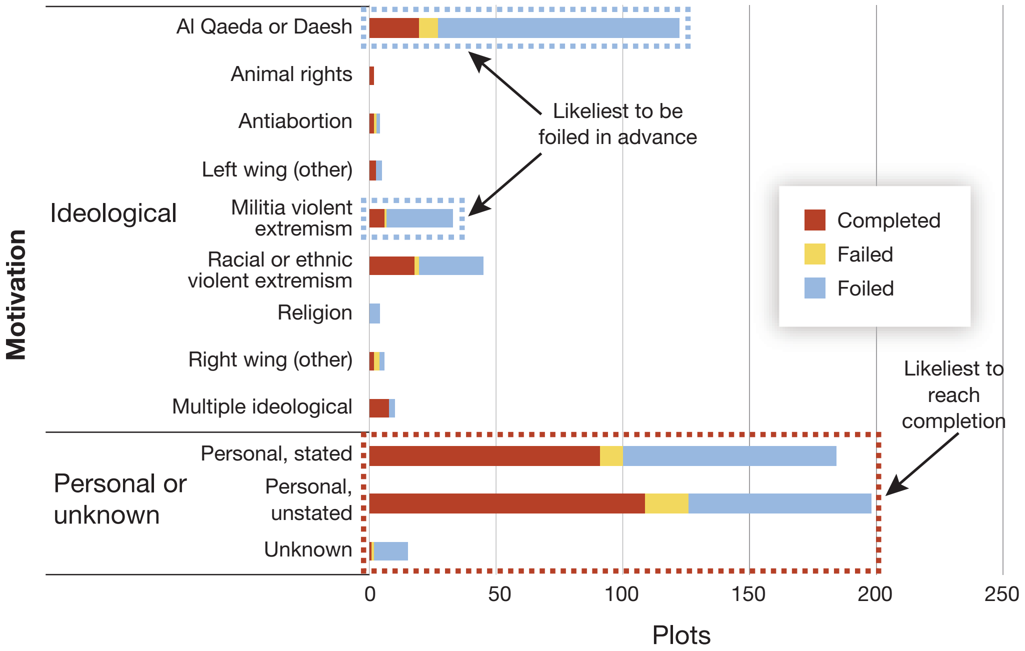
Assailant Motivations Against Soft Targets and Crowded Places

Figure 2.5 shows the total numbers of ST-CP attack plots in the MADT dataset, by motivation. As shown, the greatest number of plots by far has been for personal or unstated reasons (63 percent), followed by al Qaeda– and Daesh-related plots (19 percent), followed distantly by domestic extremist motivations (17 percent).

Plots for some of the ideological motivations—notably, al Qaeda and Daesh and militia violent extremism—were significantly likelier to be foiled in advance. This could be because of the high-profile nature of the threat actor and the visibility that the U.S. government and LE give to these actors, especially since the 9/11 terrorist attacks. In contrast, personally motivated plots were likelier to reach execution. We hypothesize that this is due to factors including the following:

- These plots tended to be more complicated and involve more people, making the chances of plot leakage or simple failure likelier.
- These plots also tend to involve outreach to external international (al Qaeda, Daesh) or domestic (militia) extremists under very heavy monitoring and investigative scrutiny,

FIGURE 2.5
Mass-Attack Plots, by Motivation



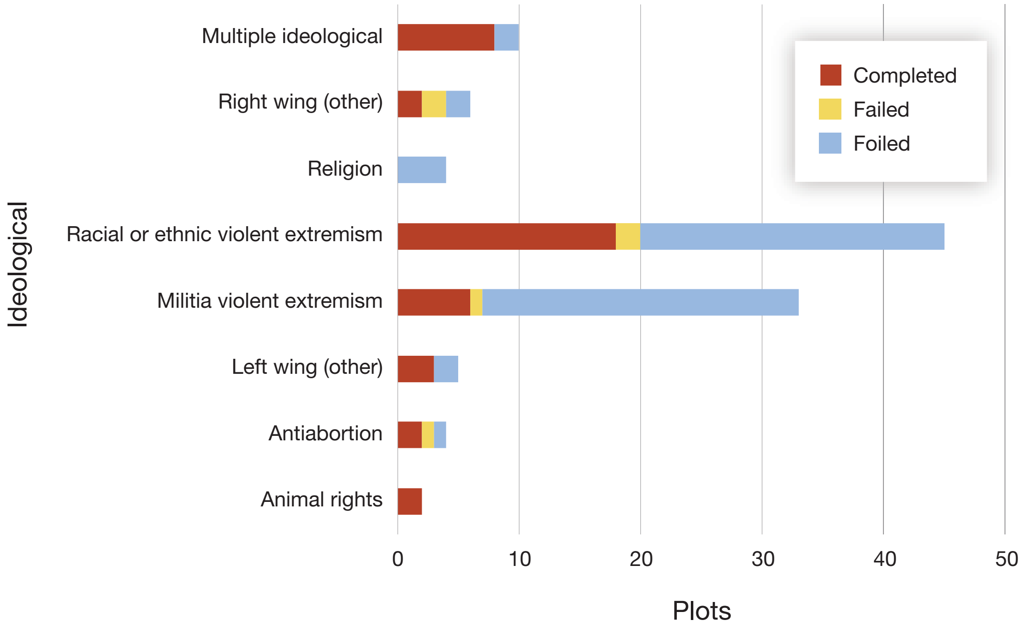
SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated all cases (*n* = 628).

making it likelier that a would-be perpetrator will be found through investigative observations of their associations and contacts with these external extremists.

- In contrast, a perpetrator planning an attack for their own personal reasons might well not speak with anyone about their motivations and intentions, making the likelihood of proceeding undetected much greater.

To provide more insight on the domestically motivated plots, which are somewhat obscured in Figure 2.5, Figure 2.6 shows just the total counts of these plots. As shown, plots motivated by racial or ethnic violent extremism and by militia violent extremism have dominated in the period covered by the MADT dataset (1995 to 2020). However, given that domestically motivated plots made up only 17 percent of the total, these are still small shares of the total set of attack plots.

FIGURE 2.6
Mass-Attack Plots with Domestic Extremist Motivations



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated all cases in the dataset that had domestic extremist motivations (*n* = 109).

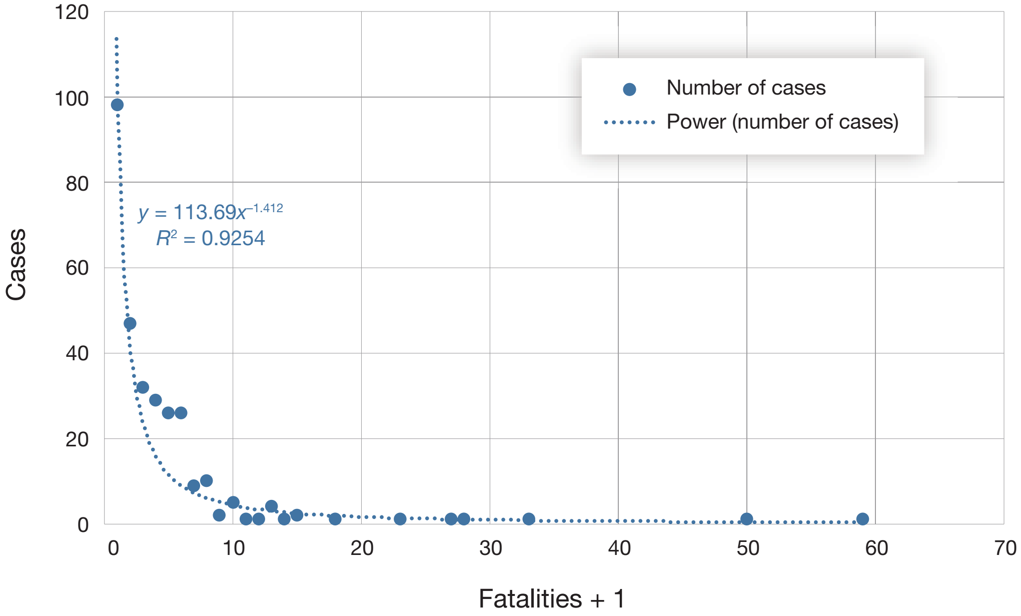
Factors Affecting Casualties

A General Characterization of Fatalities During Mass Attacks

Figure 2.7 shows the distribution of the number of attacks (reaching execution, both completed and failed) by the number of fatalities within each attack, withing the MADT dataset. As shown, higher-fatality attacks occur with consistently lower frequency than lower-fatality attacks. Most attacks have had fewer than ten fatalities; a majority had fewer than five. However, large-fatality attacks occur with much more frequency than one would expect from a "well-behaved" distribution, such as a normal distribution. Instead, a power law distribution fits the observed fatality frequencies well. A power law distribution is one in which the probabilities of an event happening are proportional to some mathematical power of the magnitude of the event—for example, the probability that an attack will have a given number of fatalities might decline with the square of the number of fatalities (so an attack with ten more fatalities is 100 times rarer). Power law distributions are consistent with would-be attackers needing to carry out a series of escalating actions without being detected or otherwise knocked back by defenders (or other obstacles) across multiple stages of an attack to success-

FIGURE 2.7

Frequency of Attacks Reaching Specified Numbers of Fatalities



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated every nonfoiled case in the dataset that had a known number of fatalities (n = 295). To permit fitting the power law curve to the data, we needed to increase all fatality accounts by 1 (because power laws technically cannot apply to zero counts). Thus, the number of attacks with zero fatalities is shown as 1, attacks with one fatality are shown as 2, and so on.

fully cause high numbers of fatalities.[8] In the landscape assessment, we leveraged this idea of would-be attackers having to complete a series of stages to develop a concept of using layers of security to defend ST-CPs more effectively and efficiently.

Figure 2.8 shows what proportions of all fatalities in the MADT dataset were due to attacks having more than ten fatalities, between five and nine fatalities, and fewer than five fatalities. As shown, each accounted for about one-third of the total fatalities. Thus, although coverage understandably tends to focus on the highest-fatality events, there is a strong need to focus also on preventing and protecting against lower-fatality attacks, given their greater likelihoods.

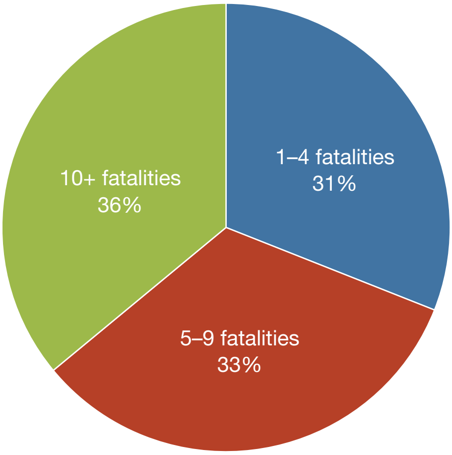
Crowds, Accessibility, and Location Types for Soft Targets and Crowded Places

Figure 2.9 shows the average number of fatalities, by type of ST-CP location. By far, the highest-fatality locations are outdoor event venues, with the average extending past the chart

[8] Bohorquez et al., "Common Ecology Quantifies Human Insurgency."

FIGURE 2.8

Percentage of Mass Attack–Caused Fatalities at Each Attack Fatality Level



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated every nonfoiled case in the dataset that had a known number of fatalities (*n* = 295).

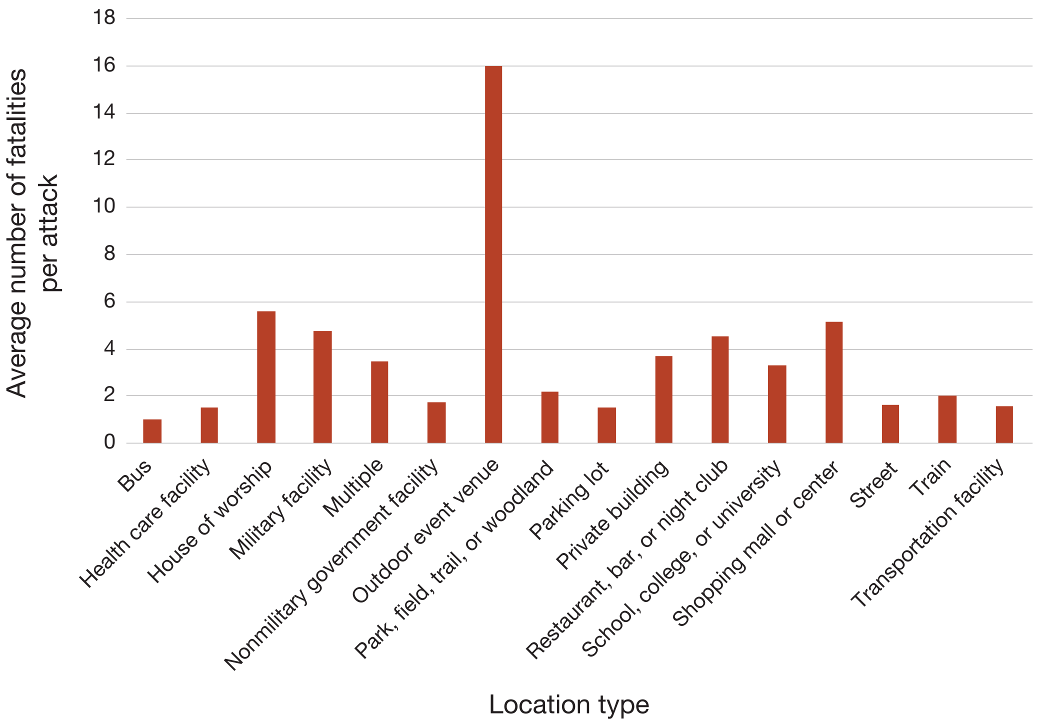
to 16 fatalities. This average is largely due to one event (the Route 91 Harvest Festival shooting in Las Vegas, with 58 fatalities) because there were only four completed outdoor event venue attacks. Other types of locations with high average numbers of fatalities include houses of worship; shopping malls; buildings on military installations; and restaurants, bars, and nightclubs.

The presence of a crowd—especially a dense crowd—was strongly associated with greater numbers of fatalities. Figure 2.10 shows that ST-CP attack locations with dense crowds present had more than twice the fatalities, on average. Unsurprisingly, the ST-CP types that tend to have denser crowds present also had higher average numbers of fatalities.

Figure 2.11 shows the total numbers of fatalities across all attacks in the MADT dataset, by location type. This reflects the average numbers of fatalities per attack (as shown in Figure 2.9) times the number of completed attacks. Thus, here we see that, to date, the biggest sources of ST-CP casualties have been attacks on private buildings (typically workplaces), followed by education facilities; restaurants, bars, and nightclubs; houses of worship; shopping malls; and streets. The first two had medium numbers of fatalities per attack but comparatively high numbers of attacks. Also of note is the number of total fatalities at outdoor event venues; these are largely due to one event (the Las Vegas music festival shooting).

FIGURE 2.9

Average Fatalities, by Location Type



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities (*n* = 262). The vertical axis is truncated at 8 so that the average numbers of fatalities at attack location types other than outdoor event venues remain visible. This figure shows only the more-frequent location types that had fatalities.

Weapons Employed and Numbers of Fatalities

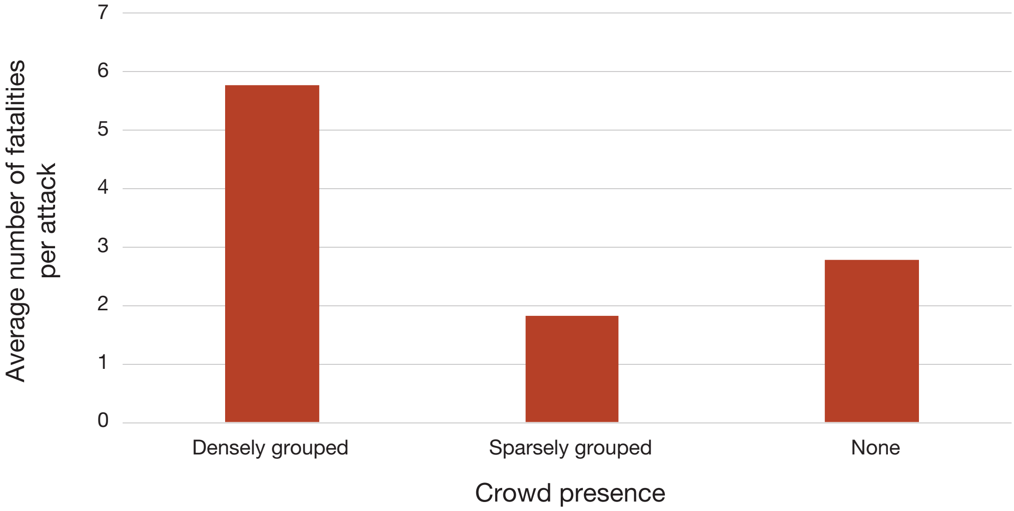
Figure 2.12 shows the average number of fatalities per attack, by type of weapon employed (or combinations of types of weapon employed). As shown, attacks with shootings had higher average numbers of fatalities than any other type of attack.

Figure 2.13 shows the total numbers of fatalities resulting from attacks involving different types of weapons during completed attacks in the MADT dataset. (We considered only completed attacks because otherwise, earlier preventions or failures limited numbers of casualties regardless of weapon choice.) As shown, the number of fatalities from shootings dominated the total, accounting for more than 90 percent of all casualties. Thus, the ST-CP attack problem is predominantly a mass-shooting problem.[9] Other modes of attack have not produced high numbers of casualties at ST-CP locations in recent years.

[9] The MADT deliberately does not include terrorist attacks from before 2002, so it excludes the 9/11 and Oklahoma City bombing attacks.

FIGURE 2.10

The Association Between Crowd Presence and Average Numbers of Fatalities



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities *(n* = 262).

We next consider, within shootings, what types of firearms produced the highest average and total numbers of fatalities. Figure 2.14 shows both the total numbers of fatalities from employing different types of firearms (including no firearms) and the average numbers of fatalities per completed attack.

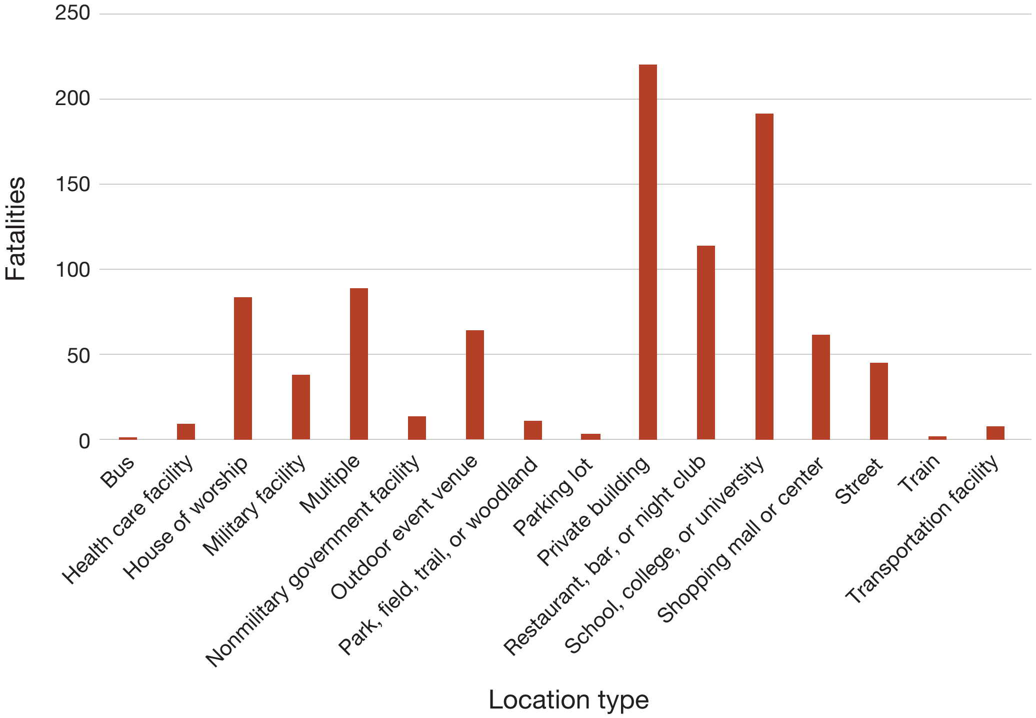
As shown, the main differentiators for attack lethality were first, whether guns were used, and second, whether multiple guns were used. There was not much difference in average numbers of fatalities between using a single rifle (such as an AR-15) or a handgun (such as a 9 mm) in the mass-attack data.

The comparative prevalence of using handguns further meant that the biggest share of all attack fatalities was from handguns, followed by attacks using multiple guns. Use of a rifle was in third place for total fatalities.

In one attack—the Las Vegas festival shooting—the perpetrator used multiple rifles retrofitted to fire automatically. That one attack resulted in 58 fatalities. It is a single case and an outlier and is thus not included in Figure 2.14.

The mode of firearm acquisition was also considered, although the lack of acquisition information for many cases limits interpretability. We excluded foiled cases from this analysis (because many cases had not matured to the stage of weapon acquisition and there was only limited reporting on the acquisition method in these cases). Of the 241 nonfoiled cases that involved one or more firearms, weapon acquisition information was readily available for 110 (46 percent). Firearms were illegally acquired in 39 incidents and legally acquired in 71 inci-

FIGURE 2.11
Total Numbers of Fatalities, by Location Type



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities (*n* = 262).

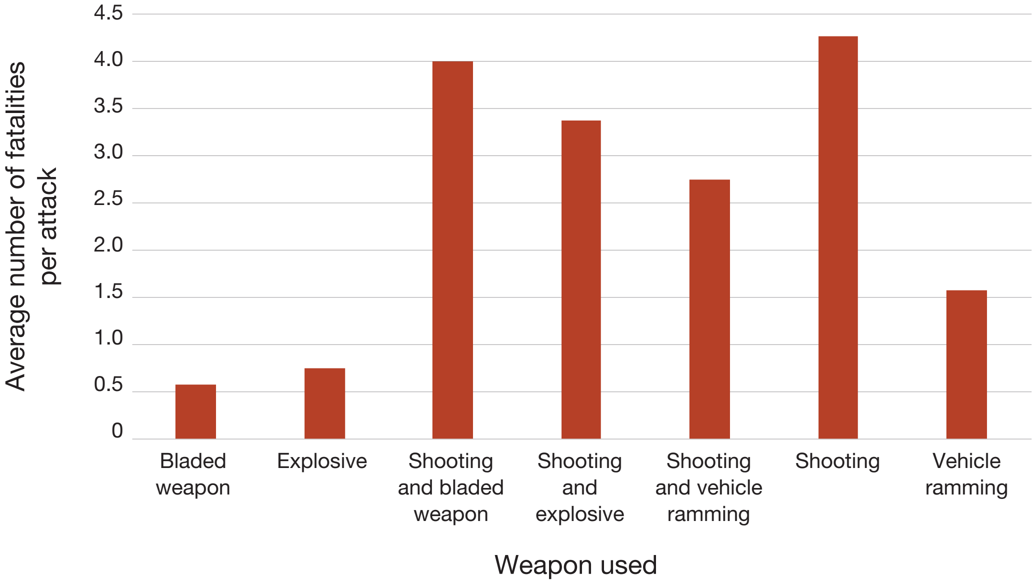
dents of the remaining cases, with a large majority of the latter being through regular purchases from federally licensed firearm dealers.

In this chapter, we have explored several key aspects of the ST-CP landscape. The type of threat actor has changed in the past 30 years, from more–ideologically driven threat actors to ones with more-personal grievances against specific groups or polygrievances that combine grievances and coalesce in an act of violence. Schools and other education facilities have been targeted the most, but private buildings, government facilities, houses of worship, open streets, and restaurants, bars, and nightclubs have also seen significant numbers of attacks. The number of attacks per geographical area appears to track with population, with New York City and Washington, D.C., being notable exceptions.

Like with the number of attacks, attacks on schools and private buildings had the highest average numbers of fatalities, with fatalities involving firearms, either solely used or in combination with other weapons, causing the most fatalities both in total number and in average number per attack. In the firearm realm, handguns caused the most fatalities. Chapter 3 describes the literature on protective measures and examine how such measures foil attacks, identifying real-world examples through the analysis of multiple AARs and case studies.

FIGURE 2.12

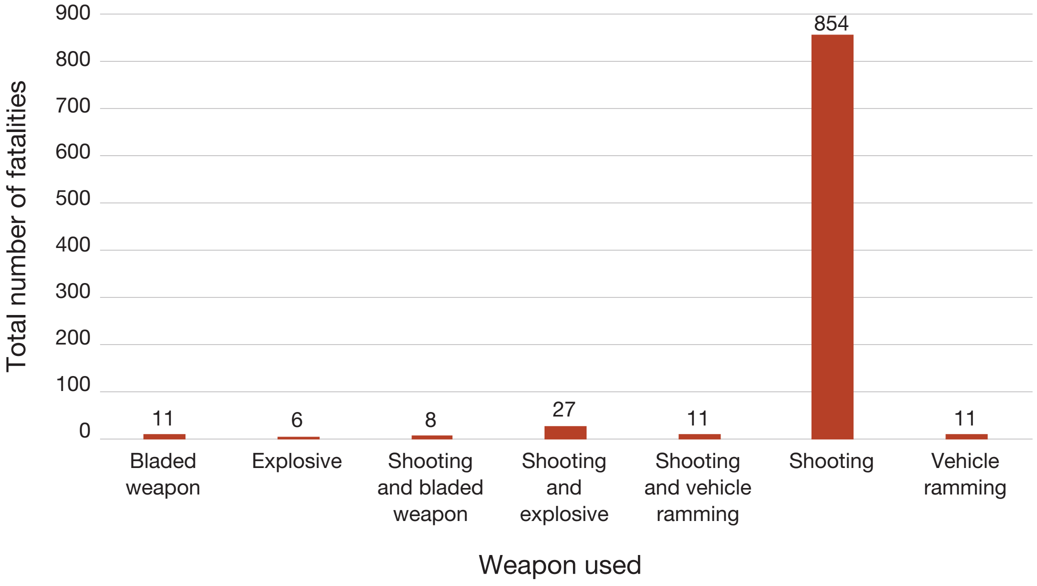
Average Numbers of Fatalities, by Type of Weapon Used



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities (*n* = 262).

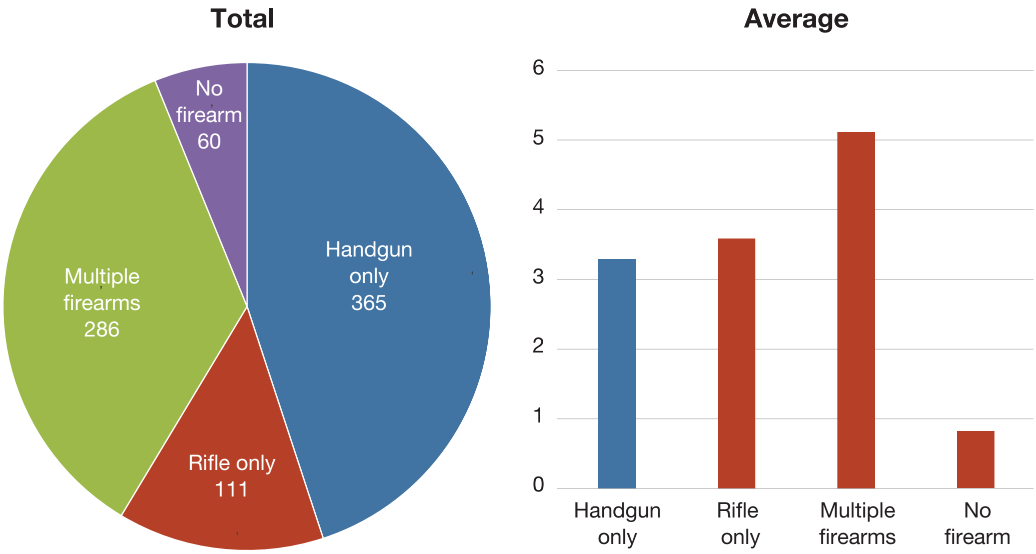
FIGURE 2.13
Total Numbers of Fatalities, by Type of Weapon Used



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities (*n* = 262).

FIGURE 2.14

Total and Average Numbers of Fatalities from Attacks Involving Different Types of Weapons



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated every completed case in the dataset that had a known number of fatalities but excluded the Las Vegas festival shooting case (*n* = 261).

CHAPTER 3

Assessing Preventive and Protective Measures

Common Preventive and Protective Measures and Strategies: Results from the Literature Review

As noted in Chapter 1, 166 sources identified in our literature review—including AARs—were coded as either highly or moderately relevant to this study; the discussion of literature review results in this chapter draws on these sources, relying primarily on the 78 sources coded as highly relevant and, to a lesser extent, on the 88 sources identified as moderately relevant.

Our review identified primarily sources discussing protective measures for the K–12 school sector, followed by measures and strategies applied to enhance physical security at major events and CPs (e.g., sporting events, concerts) and at transportation and mass-transit facilities. We also identified a set of sources that generally addressed the use of protective measures across various types of ST sectors and a smaller number that focused specifically on houses of worship and health care facilities. Our searches revealed that the fewest sources were specific to protests and demonstrations.

Across these sectors, protective measures have various intended benefits. A common goal of implementing security measures is to reduce the likelihood of a physical attack and associated harm. Certain strategies aim to reduce the likelihood of attacks perpetrated by outsiders (e.g., fencing, door locks), while others aim to reduce the likelihood of insider attacks (e.g., drug-sniffing dogs, LE and other security personnel).[1] Across many sectors, various response strategies have also been adopted to thwart or minimize the impact of active shooters.[2]

[1] The quantitative analysis provided in Chapter 2 did not address insider versus outsider threat as a factor in target location because the underlying data sources did not identify this as a variable.

[2] Arteaga and Park, “Building Design and Its Effect on Evacuation Efficiency and Casualty Levels During an Indoor Active Shooter Incident”; Doss and Shepherd, *Active Shooter*; Gundry, “Physical Security Design and the Active Shooter”; King and Bracy, “School Security in the Post-Columbine Era”; Reeping et al., “Rapid Response to Mass Shootings”; Zhu et al., “Building Preparedness in Response to Active Shooter Incidents.”

Many of the sources identified in our review that were general to ST protection addressed specifically defending against, mitigating, and responding to active-shooter or active-assailant attacks. Various sources—peer-reviewed academic studies, non–peer-reviewed reports, and guidance from federal agencies—provide insight into strategies to reduce the lethality of, respond to, and, to a lesser extent, prevent such incidents. For example, studies focused on reducing casualties during active-shooter events highlight the potential impact of architectural features (building exit width, door width, and hallway width) that facilitate more-efficient evacuations.[3] Other studies have shown that one of the most–commonly referenced protective measures for active-shooter incidents is access control generally speaking, which can include reducing the number of entrances into a building, posting someone at a reception or security desk near a main entrance, access control badges, and metal detectors.[4]

Layered security is another frequently mentioned approach to detecting, delaying, and responding to active-shooter incidents. Integrating zones into the outer and inner layouts of a facility (e.g., the outdoor areas of a school campus and the perimeters and interiors of school buildings) can help to prevent single points of failure by ensuring that measures in place across zones reinforce one another.[5] Communication technologies, including mass-notification systems, are also common countermeasures to mitigate active-assailant attacks across physical security layers, as are regular training and drill protocols for building occupants, bystanders, and first responders.[6]

Sources that emphasize the role of architectural design in responding to active-assailant attacks have said that such approaches can integrate diverse security measures while still preserving the "function and aesthetics of buildings."[7] Crime prevention through environmental design (CPTED), for instance, uses a combination of design, technology, and personnel and management to deter violence and crime across various ST types.[8] CPTED principles integrate strategies of natural surveillance (i.e., increasing awareness of who is present through strategically placed windows, lighting); natural access control (i.e., inhibiting potential attackers' or criminals' ability or desire to access an area through real or perceived bar-

[3] Arteaga and Park, "Building Design and Its Effect on Evacuation Efficiency and Casualty Levels During an Indoor Active Shooter Incident."

[4] Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[5] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[6] Doss and Shepherd, *Active Shooter*; Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Reeping et al., "Rapid Response to Mass Shootings"; Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[7] Gartenstein-Ross and Lahnert, "Crisis Architecture."

[8] Arnold and Lasch, *Site and Urban Design for Security*; Global Programme on Countering Terrorist Threats Against Vulnerable Targets, *Protecting Vulnerable Targets from Terrorist Attacks*; Hesterman, *Soft Target Hardening*; Králová, Šoltés, and Kotalová, "Protection of Transport Terminals Through the Application of the CPTED Concept."

riers, such as gates, fences, or foliage); and territorial reinforcement (i.e., discouraging crime and violence through design features, such as curved driveways, hallways, or landscaping) and are increasingly used to mitigate active-assailant incidents, terrorist violence, and other types of mass attacks.[9]

A related paradigm identified in our literature review is reliance on principles of situational crime prevention (SCP).[10] SCP focuses on how people capitalize on situational opportunities to commit a crime; intervening mechanisms are therefore designed to manipulate environments by increasing both the risk and effort required to successfully engage in criminal activity, ultimately reducing opportunity in the overall environment.[11] Various measures considered to be SCP techniques—such as entry control measures, lockdowns, and security personnel—have worked to successfully stop active-assailant attacks. One report, for instance, highlights the role that door locks played in denying attackers access to a targeted location and how lockdowns reduced the number of casualties during an active-assailant attack.[12] Other studies highlighting the role of SCP discuss how protective measures, such as bollards, fences, and other reinforced barriers, can help protect crowds in outdoor spaces from vehicular attacks.[13] SCP approaches to enhancing physical security across ST sectors show that various safety procedures—such as hardening targets, adding security personnel, and practicing responses to attacks—can effectively restrict an attacker's ease of movement and reduce the number of available targets, ultimately mitigating the overall level of harm caused by an incident.

Finally, some sources emphasize the importance of system-based approaches to physical security for ST environments. System-based approaches emphasize that individual elements (e.g., a closed-circuit television [CCTV] camera) are part of a broader physical security system made up of other interconnected elements; these must all function together to provide maximum security benefits.[14] Notably, the approach conceptualizes a physical security system as a combination of protective measures and technology, site design features, personnel, policies, and training programs. Each element works individually and in conjunction with other elements to detect, delay, and respond to threats and incidents.[15] In other words, SCP posits that technology should be incorporated into a comprehensive framework that includes nontechnological interventions, extensive planning and training, and rigorous evaluation against the needs of the specific facility in question. Without proper policies, training,

[9] Gartenstein-Ross and Lahnert, "Crisis Architecture."

[10] Freilich, Gruenewald, and Mandala, "Situational Crime Prevention and Terrorism."

[11] Freilich and Newman, "Situational Crime Prevention."

[12] Silva and Greene-Colozzi, "What We Know About Foiled and Failed Mass School Shootings."

[13] Williams, Corner, and Taylor, "Vehicular Ramming Attacks."

[14] Gundry, "Physical Security Design and the Active Shooter."

[15] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

and planning, technologies will be less likely to meet the safety and security requirements of a specific facility.[16]

What Does the Literature Cover Across Sectors?

Our review of the literature on protective measures across diverse ST sectors suggests that surveillance technology (e.g., CCTV systems), interior and environmental design strategies, and physical barriers are the most-referenced measures. Table 3.1 shows the types of protective measures commonly referenced in each sector; the subsequent sections describe specific approaches identified in the literature for each sector in more detail.

Protective Measures in K–12 Schools

Schools use a multitude of measures to ensure the safety and security of their communities. Various researchers have categorized measures according to different criteria, including their intended functions, their visibility, and distinctions between what counts as a measure versus what counts as a policy. Taking the first approach, for instance, Schwartz and her coauthors organized school safety technologies into the following categories:[17]

- entry control equipment (e.g., electromagnetic door locks, mobile barricades)
- identification (ID) technology (e.g., student and staff IDs, visitor badges)
- video surveillance technology (e.g., CCTV, motion-sensor systems)
- communication technology (e.g., two-way staff radios, phones)
- alarms (e.g., motion and heat detectors, scream alarms)
- emergency alerts (e.g., automated text messages or emails)
- metal detectors
- anonymous tip lines
- tracking systems (e.g., smartphone applications)
- school bus route maps
- violence prediction technology
- social media monitoring tools.

Those who group security measures according to their visibility focus especially on those that are seen by students and school staff on a daily basis, such as metal detectors, CCTV, and school police or other uniformed security personnel.[18] Others focus on the simultane-

[16] Interagency Security Committee, *Best Practices for Planning and Managing Physical Security Resources*; Johns Hopkins University Applied Physics Laboratory, *A Comprehensive Report on School Safety Technology*; Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Research and Special Programs Administration, *Transit Security Design Considerations*.

[17] Schwartz et al., *The Role of Technology in Improving K–12 School Safety*.

[18] Addington, "Cops and Cameras"; Jonson, "Preventing School Shootings"; Tanner-Smith et al., "Adding Security, but Subtracting Safety?"

TABLE 3.1

Overview of Commonly Referenced Protective Measures for Soft Targets

Measure	K–12 Schools	Mass Transit	CPs	Major Events	Houses of Worship	Health Care	Protests
Access points			x				
Barriers		x	x		x		
CCTV	x	x		x			
Detection technology[a]	x	x		x	x	x	
Door systems	x						
Entry screening	x					x	
Environmental design[b]			x				x
Interior design[c]						x	
LE		x	x	x	x		x
Place management[d]					x		
Security personnel				x			
Signage						x	

[a] Such measures as metal detectors, gunshot detection systems, and motion-sensor technology.

[b] Design in outside areas (e.g., landscaping).

[c] Design inside buildings (e.g., curved hallways, small windows).

[d] The presence of dedicated personnel to provide security.

ous implementation of specific security measures (e.g., cameras and door locks) and associated policies (e.g., door policies and visitor sign-in processes).[19] These distinctions are logical insofar as they help capture the different implementation and longer-term maintenance costs of various measures (for instance, around hiring school police officers, such as SROs, or purchasing specific equipment, such as cameras), as well as the training demands associated with specific policies (e.g., lockdown drills to practice locking classroom doors in the event of an emergency). Indeed, many protective measures and technologies are unlikely to offer their full security benefits without appropriately trained personnel to operate and maintain them and policies in place to dictate how they will be used on a day-to-day basis and during emergency situations.[20]

NCES provides annual statistics on the preventive and responsive measures that schools have put in place to promote discipline and enhance school safety. The 2021 report, which provides statistics on the 2019–2020 school year, shows that 90 percent of public schools in the United States had a written emergency preparedness plan to address active-shooter situations, bomb threats, and other types of hazards.[21] During that same school year, more than 90 percent of public schools also reported controlling access to buildings during school hours and using security cameras to monitor school grounds and buildings; more than 70 percent required faculty and students to carry badges or photo ID.[22] By contrast, less than 10 percent of public schools reported conducting random metal detector checks. More-recent surveys conducted by the Institute of Education Sciences' (IES's) School Pulse Panel also show that 52 percent of public schools reported having any sworn LE officers, including SROs, on campus at least once a week during the 2022–2023 school year and that school personnel largely agreed that security personnel (SROs, security officers, or sworn LE officers) made a positive impact on their school community.[23] A HSOAC survey fielded in October and November 2022 to a nationally representative sample of 973 K–12 school teachers largely corroborates these findings: Nearly all teachers worked in schools that had a least one security measure, the most common of which were visitor systems, exterior and interior door locks, and staff ID badges.[24] Teachers' responses suggest that metal detectors continue to be a less

[19] Perumean-Chaney and Sutton, "Students and Perceived School Safety."

[20] King and Bracy, "School Security in the Post-Columbine Era"; Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

[21] Irwin et al., *Report on Indicators of School Crime and Safety*.

[22] NCES, "Fast Facts."

[23] IES, "School Pulse Panel." Survey results indicate that between 59 and 69 percent of schools strongly agreed that SROs, security officers, or sworn LE officers "make a positive impact on our school community" (IES, "School Pulse Panel").

[24] Jackson, Diliberti, et al., *Teachers' Views on School Safety*.

commonly used protective measure, although results also show that these are more common in schools serving historically underrepresented student populations.[25]

Protective Measures in Transportation and Mass Transit

In the transportation sector, physical security measures are implemented to reduce vulnerabilities associated with various threats, such as everyday crime and rarer instances of terrorist attacks. Common security countermeasures that provide security benefits by preventing and deterring attacks include police or security personnel; visible surveillance systems, such as CCTV cameras; passenger and baggage screening procedures; physical barriers; PA systems; and signage.[26] Many of these measures, such as security personnel, surveillance systems, and PA systems, also provide capabilities for responding to incidents, alongside training regimens, information-sharing, and other protocols and policies.

Various sources of guidance for the transportation sector emphasize the importance of implementing a layered approach to physical security, in large part to avoid having single points of failure.[27] Guidance also draws on the concepts of a system-based approach to security, which emphasizes integration across the full set of measures designed to prevent, deter, detect, mitigate, respond to, and recover from attacks.[28] Transit agencies of different sizes also face different threats, can devote varying levels of resources to security, and thus have different security requirements.[29] As is true for schools, such variation emphasizes that there is no one-size-fits-all solution to promoting physical security across a diverse set of mass-transit agencies; guidance recommends that site planners, security directors, and other stakeholders account for their unique contexts and needs when making decisions about protective measures and any associated policies and training.

[25] Jackson, Diliberti, et al., *Teachers' Views on School Safety.*

[26] National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; Transit Cooperative Research Program; et al., *Policing and Security Practices for Small- and Medium-Sized Public Transit Systems.*

[27] National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; National Cooperative Highway Research Program; et al., *Update of Security 101*; National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; Transit Cooperative Research Program; et al., *Policing and Security Practices for Small- and Medium-Sized Public Transit Systems.*

[28] National Academies of Science, Engineering, and Medicine; Transportation Research Board; Transit Cooperative Research Program; et al., *Policing and Security Practices for Small- and Medium-Sized Public Transit Systems*; National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; National Cooperative Highway Research Program; et al., *Update of Security 101.*

[29] National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; Transit Cooperative Research Program; et al., *Policing and Security Practices for Small- and Medium-Sized Public Transit Systems.*

Protective Measures in Crowded Places and Major Events

The literature that we identified as specific to CPs and major events takes a more general approach to physical security in STs and largely encompasses studies and guidance related to sports stadiums, shopping malls, and bars and restaurants. Federal guidance specifies that, "by the nature of their purpose [these facilities] do not incorporate strict security measures" compared with those of some other ST sectors (such as airports).[30] Relevant sources describe various protective measures used to promote security in such spaces, as well as strategies for crowd management and increasing awareness among facility employees and patrons. The protection of CPs often relies on both design features and place management. Some people have argued that "safety through design" is more appropriate than so-called procedural safety, which can be subject to human error.[31] Designs for CPs might therefore focus on avoiding hazards created by inadequate walkway and stair design, the presence of uneven walking surfaces, mixing vehicles with people, and two-way systems, such as roads.[32] Other strategies related to facility design include the concepts of defense in depth (establishing standoff distance around buildings, for example, with hardened and appropriately designed seating, lighting posts, and signs), defense in structure (using resilient materials resistant to ballistic or explosive attack in the construction of doors, windows, and facades), and defense within (separating employees and visitors, for example, by limiting or separating entry points or integrating efficient screening processes).[33] Notably, studies of patrons' reactions to visible security measures in CPs also suggest that such measures as fencing, CCTV cameras, and uniformed security personnel elicited positive responses and reinforced perceptions of safety.[34]

Federal and other guidance in the United States also encourages facility managers, security personnel, and other stakeholders to develop relationships with local LE and other first responders to share information about any planned large events, including details about venue layout and any established roles and responsibilities related to emergency response.[35] Developing plans for security and emergency response and communications is also critical to mitigating attacks, as is training all staff and volunteers on the basics of security, emergency protocols, and the importance of staying aware of suspicious behavior.[36] Security plans should be considered living documents: They should remain flexible enough to integrate

[30] Cybersecurity and Infrastructure Security Agency (CISA), *Security of Soft Targets and Crowded Places*.

[31] Ancliffe, "Crowd Planning for Public Safety."

[32] Ancliffe, "Crowd Planning for Public Safety."

[33] Peck, "Security and Democracy."

[34] Dalgaard-Nielsen, Laisen, and Wandorf, "Visible Counterterrorism Measures in Urban Spaces."

[35] Bigda, "Strategies for Crowd Management Safety"; Connors, *Planning and Managing Security for Major Special Events*; DHS, "Mass Gatherings."

[36] DHS, "Mass Gatherings."

and leverage new resources and information.[37] Studies show that casualty rates from active-shooter incidents decrease with LE response times.[38] In addition, the fact that rates of police officers' shooting accuracy are higher stresses the importance of training for LE personnel that centers on mass attacks in CPs.[39]

Protective Measures in Houses of Worship and the Health Care Sector

Most of the literature included in our review that was specific to houses of worship came from federal agencies and focused on preventing and mitigating active-assailant attacks. CISA emphasizes the need to take a comprehensive and multilayered approach to defending such spaces, integrating measures at a facility's outer perimeter (e.g., solar or timed street lights, fencing and gates, landscaping, video surveillance), building perimeter (e.g., reinforced doors and windows, video surveillance, alarm systems, and access control measures), and inner perimeter (e.g., visitor management systems and policies, access control measures, alarms, and an active-shooter preparedness program for congregants).[40] Although some visible security measures could be perceived as unwelcoming or drastic in some settings, others—such as a welcoming committee that includes people trained to identify suspicious activity—are likelier to go unnoticed and cause less disruption to a facility's intended purpose.[41]

Studies and guidance specific to hospitals and health care facilities also focused largely on active-assailant attacks. We identified specific points of emphasis around the importance of sharing information with first responders and training staff on various active-assailant responses.[42] Sources have identified emergency departments, outpatient clinics, parking lots, patient rooms, and intensive care units (in that order) as the most common locations for shootings at health care facilities and offer guidance on safe design strategies to help deter and prevent attacks.[43] Key strategies include adding uniformed security personnel to facility entrances and ensuring that their presence is visible; integrating additional screening for patrons, such as metal detectors or wands, where appropriate; a reception desk that allows interaction with patients while providing the means for early notification of an emergency

[37] National Center for Spectator Sports Safety and Security, *Interscholastic Athletics and After-School Safety and Security*.

[38] National Center for Spectator Sports Safety and Security, *Interscholastic Athletics and After-School Safety and Security*.

[39] Lee, Ostrowski, and Dietz, "Effectiveness of Unarmed Response to Active Shooter Incidents."

[40] CISA, *Mitigating Attacks on Houses of Worship*.

[41] Houses of Worship Committee, "Recommended Best Practices for Securing Houses of Worship Around the World."

[42] Healthcare and Public Health Sector Coordinating Council, *Active Shooter Planning and Response*; Healthcare and Public Health Sector Coordinating Councils Public Private Partnership, *Active Shooter Planning and Response in a Healthcare Setting*.

[43] Schwerin, Thurman, and Goldstein, "Active Shooter Response."

(e.g., through a panic button); and ensuring that each facility has a clear lockdown policy and that facility staff are trained on such policies.[44]

In all these sectors, the sources that we reviewed stressed the dilemma that STs face in promoting security while maintaining an aura of openness and a welcoming environment generally; in schools, transportation hubs, houses of worship, retail stores, stadiums, and hospitals, public access is critical to daily operations and fulfills key missions.[45] The physical security planning process is therefore a complex one.[46] Adopting a system approach—one that is flexible, scalable, and integrates security measures and technology alongside personnel, site design considerations, policies, and training—is promising for helping address some of these challenges.[47]

Insight from Incident After-Action Reports

Overall, the AARs we examined as part of our literature review focused minimally on protective measures; most reports focused primarily on multiagency responses to mass-attack events. Both of the AARs that did address protective measures and their impact on incident outcomes in detail covered mass shootings at K–12 schools (the shooting at MSDHS in Parkland, Florida, in 2018 and the shooting at Robb Elementary School in Uvalde, Texas, in 2022). In the case of the Police Foundation's AAR covering the shooting at MSDHS, a critical lesson learned focused on the facility's CCTV camera system, which was running on a delay at the time of the incident.[48] The delay was unbeknownst to school staff, including security personnel, and ultimately complicated emergency response: LE believed the shooter to be in a building in which he was not during the incident and received erroneous information about his location once he had left campus.[49] A second report covering the incident and authored by the MSDHS Public Safety Commission highlights additional physical security failures that led to higher casualty levels that were related specifically to the absence of effective security measures at the campus and building perimeter layers, the inability to lock classroom doors from inside, glass sections in classroom doors, the absence of PA speakers in common areas of the school building, conflicting alarm systems, and inadequate policies and training on lockdown procedures.[50]

[44] Huddy, "Design Considerations for a Safer Emergency Department."

[45] Research and Special Programs Administration, *Transit Security Design Considerations*.

[46] Steiner et al., *Challenges in Implementing Physical Security Measures in K–12 Schools*.

[47] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Research and Special Programs Administration, *Transit Security Design Considerations*; Steiner et al., *Challenges in Implementing Physical Security Measures in K–12 Schools*.

[48] Straub et al., *Recovering and Moving Forward*.

[49] Straub et al., *Recovering and Moving Forward*.

[50] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President*.

According to a commission convened following the mass shooting at Robb Elementary School, similar points of failure contributed to high casualties during that attack. Specifically, the 5-foot fence at the school's outer perimeter did not stop the attacker, and at least one exterior door was propped open on the day of the incident. The report also cites regular noncompliance with door policies, which left occupants more vulnerable to attack.[51] Moreover, the frequency of emergency alerts and campus lockdowns resulting from police operations against human traffickers in the vicinity of the school contributed to a culture of complacency among school staff. Any alarms and notifications sent out on the day of the attack did not instill the necessary sense of urgency among staff, including security personnel.[52]

Other AARs discuss the role of protective measures in less detail but provide important lessons learned, nonetheless. Most of these lessons center on improving protective measures or enhancing preparedness to enable more-effective LE responses to active-assailant attacks. For example, an AAR from the 2012 shooting at Sandy Hook Elementary School in Newtown, Connecticut, recommends providing emergency responders with building schematics, master key sets, and other resources in advance to improve response.[53] Other AARs similarly recommend staging specific equipment, such as tactical vehicles, shields, and other gear, in proximity to STs to enable quicker and more-effective LE response to emergencies.[54] (This recommendation presumes that the location is facing a sufficient threat to make prestaging the equipment worthwhile, given limited resources.) The importance of careful physical security planning and training for active-assailant attacks was also emphasized in multiple AARs: Prior completion of a physical security survey could have alerted personnel to critical vulnerabilities and identified areas for additional protection in some targeted facilities.[55] Other common recommendations included ensuring that facility employees and volunteers are up to date on active-shooter training and that they and facility patrons are familiar with how to recognize and report suspicious behavior.[56]

Finally, the AARs we reviewed provide some recommendations for improving protection for large outdoor events, including mass protests and demonstrations. New video technology, such as aerial footage from drones, can improve surveillance of such events and aid in

[51] Investigative Committee on the Robb Elementary Shooting, *Interim Report 2022*.

[52] Investigative Committee on the Robb Elementary Shooting, *Interim Report 2022*.

[53] Connecticut State Police, *After Action Report*.

[54] Clark County Fire Department, Las Vegas Metropolitan Police Department, and National Exercise Division, *1 October After-Action Report*.

[55] Chief of Naval Operations, "Investigation into Fatal Shooting Incident on Naval Air Station Pensacola of 6 December 2019"; Hillard Heintze, *The City of Virginia Beach*. Significant sections of the report on the Naval Air Station Pensacola shooting, including those detailing the installation's critical vulnerabilities and recommendations for corrective actions, have been redacted from publicly available versions.

[56] Chief of Naval Operations, "Investigation into Fatal Shooting Incident on Naval Air Station Pensacola of 6 December 2019"; Hillard Heintze, *The City of Virginia Beach*; Massachusetts Emergency Management Agency et al., *After Action Report for the Response to the 2013 Boston Marathon Bombings*.

response in the event of an emergency.[57] Protests and large events held in stadiums benefit from having a secure outer perimeter that is large enough to accommodate large crowds (including crowds that have the potential to become confrontational) and fixed checkpoints that allow safe entry and exit.[58] Barricades—including emergency vehicles and specific landmarks—can also help demarcate zones within a perimeter to facilitate crowd control.[59]

The remaining themes identified in the AARs included in our review center largely on cross-agency coordination and leadership and communications during mass-attack events.

Because of the scale and rapid evolution of mass attacks in public spaces, unified or single incident commands overall were often not established quickly or efficiently. In many of the incidents covered in our sample of AARs, the lack of clear leadership impeded response.[60] Moreover, failure to designate specific roles and responsibilities for appropriate leaders and agencies involved in response often overwhelmed responders, who did not have a clear idea of what the division of labor would look like.[61] This lack of coordination frequently resulted in delayed response times and confusion about how to coordinate key activities, including establishing a command post and staging area, dispatching and deploying appropriate resources, and treating and evacuating casualties. The self-deployment of first responders also often added to this confusion and highlighted the necessity of better adapting to and anticipating an influx of first responders during such attacks.[62] In some cases, including the one at Robb Elementary, a lack of clear leadership and coordination across multiple agencies interrupted the flow of information.[63]

Indeed, the lack of efficient communications between first responders was a predominant theme throughout the AARs we reviewed. Responses were often negatively affected by overcrowded channels, lack of access to the appropriate radio channels, faulty Wi-Fi connections, a lack of charging equipment for cell phones and radios, and the use of other ineffective

[57] National Police Foundation, *Preparing for and Responding to Mass Demonstrations and Counter-Demonstrations in Portland, Oregon*.

[58] National Police Foundation, *Preparing for and Responding to Mass Demonstrations and Counter-Demonstrations in Portland, Oregon*.

[59] Los Angeles Police Department, *An Examination of May Day 2007*; National Police Foundation, *Preparing for and Responding to Mass Demonstrations and Counter-Demonstrations in Portland, Oregon*.

[60] Broward County Aviation Department, *Fort Lauderdale–Hollywood International Airport Active Shooter Incident and Post-Event Response January 6, 2017*; Investigative Committee on the Robb Elementary Shooting, *Interim Report 2022*; Leonard et al., Why *Was Boston Strong?* National Police Foundation, *After-Action Review of the Orlando Fire Department Response to the Attack at Pulse Nightclub*; Straub et al., *Recovering and Moving Forward*.

[61] Clark County Fire Department, Las Vegas Metropolitan Police Department, and National Exercise Division, *1 October After-Action Report*; Connecticut State Police, *After Action Report*; National Police Foundation, *After-Action Review of the Orlando Fire Department Response to the Attack at Pulse Nightclub*.

[62] Braziel et al., *Bringing Calm to Chaos*; Las Vegas Metropolitan Police Department, *1 October After-Action Review*.

[63] Investigative Committee on the Robb Elementary Shooting, *Interim Report 2022*.

equipment that hindered interoperability.[64] These inefficiencies obstructed the transfer of necessary intelligence during responses to attacks, leaving emergency responders largely in the dark about key details, such as building layouts. Communication failures also hampered tracking the movement of LE personnel responding to attacks inside buildings and identifying which buildings or areas had already been swept.[65] In some cases, emergency responders relied on information coming from the public to track an attacker's movements, through such platforms as 911 calls and social media.[66]

To address these and potential other challenges, AARs emphasized the importance of following various guidelines from the National Incident Management System (NIMS), which informs how government, nongovernmental, and private organizations can work together to prevent, protect against, mitigate, respond to, and recover from incidents.[67] Establishing a unified framework and language for coordinating responses and specifying preestablished chains of command and personnel roles were common recommendations.[68] In fact, the existence of mutual-aid agreements and well-established interagency relationships prior to incidents helped speed a more efficient response in some cases.[69] Multiagency tabletop exercises and other joint exercises can ensure that different levels of LE, emergency medical services, and other agencies are better prepared to respond to active-shooter events and other emergencies when they occur.

The Effectiveness of Protective Measures and Gaps in Knowledge

Evidence about the effectiveness of protective measures for preventing, mitigating the outcome of, and responding to attacks against STs is largely inconclusive and heavily context-dependent. What little evidence does exist is based primarily on anecdotal evidence or descriptive analysis and often yields mixed conclusions.

The relatively few sources included in our review that discuss the effectiveness of protective measures across various contexts took different approaches to doing so. We did not identify any studies that employed experimental designs and only a handful that used quasi-experimental methods. Most took a largely descriptive approach to examining effectiveness, providing overviews of available technologies and measures; conducting case studies about

[64] Investigative Committee on the Robb Elementary Shooting, *Interim Report 2022*; Los Angeles Police Department, *An Examination of May Day 2007*; Metropolitan Police Department Internal Review Team, *After Action Report*; TriData Division, *Aurora Century 16 Theater Shooting.*

[65] Braziel et al., *Bringing Calm to Chaos.*

[66] Massachusetts Emergency Management Agency et al., *After Action Report for the Response to the 2013 Boston Marathon Bombings.*

[67] FEMA, "National Incident Management System."

[68] TriData Division, *Aurora Century 16 Theater Shooting.*

[69] National Police Foundation, *After-Action Review of the Orlando Fire Department Response to the Attack at Pulse Nightclub.*

their use in specific settings; and, in some cases, outlining how various aspects of the physical security planning process could increase the potential for technologies to provide security benefits (without actually testing specific arguments).[70] Other sources provided literature reviews of previous work addressing the effectiveness of physical security measures in specific sectors, most often concluding that more evaluative work was needed to understand the effectiveness of specific measures on outcomes and the potential unintended consequences of measures and technologies on such factors as facility climate and civil liberty and privacy interests.[71] Other sources based their findings on expert interviews.[72] Our review also identified agent-based modeling and other computer simulation techniques as increasingly common methods of evaluating effectiveness, given the impracticalities of real-life simulations for such purposes.[73]

Although these studies yielded mixed results, common themes did emerge in four broad areas. First, the effectiveness of protective measures appears to be highly dependent on context. Whether an attack is perpetrated by insiders rather than outsiders, for instance, affects the extent to which certain protective measures can successfully thwart that attack; although access control measures, such as ID badges, can help keep outside attackers out, they are largely ineffective when it comes to thwarting insider attacks.[74] The effectiveness of personnel-based security, such as increased LE, is also highly contingent on the circumstances of diverse contexts and, in some cases, has been found to only minimally or adversely affect levels of crime and violence in schools.[75] In the K–12 school context, hardening schools through the addition of either armed LE personnel or new security measures has a negligible impact on school shootings and is a less effective strategy than efforts that focus more on identifying threats and intervening early.[76]

[70] Johns Hopkins University Applied Physics Laboratory, *A Comprehensive Report on School Safety Technology*; National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; National Cooperative Highway Research Program; et al., *Update of Security 101*; Schwartz et al., *The Role of Technology in Improving K–12 School Safety*; Silva and Greene-Colozzi, "What We Know About Foiled and Failed Mass School Shootings."

[71] Addington, "Cops and Cameras"; Hanover Research, *Best Practices in School Security*; King and Bracy, "School Security in the Post-Columbine Era"; Price and Khubchandani, "School Firearm Violence Prevention Practices and Policies"; Reeping et al., "Rapid Response to Mass Shootings."

[72] Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[73] See, e.g., Arteaga and Park, "Building Design and Its Effect on Evacuation Efficiency and Casualty Levels During an Indoor Active Shooter Incident"; Lee, Ostrowski, and Dietz, "Effectiveness of Unarmed Response to Active Shooter Incidents"; and Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[74] Jonson, "Preventing School Shootings"; Rocque, "Exploring School Rampage Shootings"; Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[75] Devlin and Gottfredson, "The Role of Police Officers in Schools"; Na and Gottfredson, "Police Officers in Schools"; Owens, "Testing the School-to-Prison Pipeline."

[76] Jonson, "Preventing School Shootings"; NTAC, *Averting Targeted School Violence.*

Second, studies that address the effectiveness of specific responses to active-shooter events indicate the role that human factors play in influencing incident outcomes—specifically, occupant behavior, police response time, and attacker behavior. Researchers in one study, for instance, found that simulated scenarios in which building occupants used multioption responses, such as alert, lock down, inform, counter, and evacuate (ALICE), rather than traditional lockdown responses to an active-shooter incident experienced fewer casualties.[77] Researchers on other studies that were also based on computer simulations have noted that the number of attackers or an attacker's specific movements might also influence the effectiveness of protective measures and lead to unpredictable outcomes.[78] Such factors as occupants' levels of awareness and training, as well their ages and experiences, can also dictate whether measures will provide their intended security benefits.[79] Notably, casualty rates during active-shooter incidents significantly increase with delays in police response times, as suggested in the aftermath of recent mass shootings and through computer simulation models.[80]

Third, much of the literature that strives to address the effectiveness of protective measures focuses almost equally on such measures' impact on perceptions of safety and on the potential for unintended negative consequences. This is especially true of peer-reviewed studies that address the effectiveness and impact of security measures in K–12 schools. For instance, in a 2023 survey of more than 900 teachers across the United States, HSOAC researchers found that 95 percent of teachers believed that their schools' physical security measures had a positive or no effect on school climate (54 and 40 percent, respectively).[81] Three types of protective measures in particular—alarms connected directly to local police, security staff, and ID badges—correlated with teacher beliefs that physical safety had a positive impact on school climate. However, other sources that we identified in our review highlight the potentially negative impact that certain measures can have on school climate and on student and staff perceptions of safety, as well as the negative psychological impacts that active-assailant training and drills can have on youth populations if not implemented in age- and develop-

[77] Briggs and Kennedy, "Active Shooter," p. 173; Jonson, Moon, and Hendry, "One Size Does Not Fit All."

[78] Arteaga and Park, "Building Design and Its Effect on Evacuation Efficiency and Casualty Levels During an Indoor Active Shooter Incident."

[79] Zhu et al., "Building Preparedness in Response to Active Shooter Incidents."

[80] Hernandez and Diaz, "The Police Response at Robb Elementary Was a Failure, a Texas Official Says"; Lee, Ostrowski, and Dietz, "Effectiveness of Unarmed Response to Active Shooter Incidents."

[81] The U.S. Department of Education defines *school climate* as those conditions that influence student learning. Positive school climate involves strong relationships between students, teachers, families, the school, and the broader community; feeling safe from violence, bullying, harassment, and controlled-substance use; and the availability of appropriate facilities, well-managed classrooms, health supports, and fair and transparent discipline policies (National Center on Safe Supportive Learning Environments, "School Climate Improvement").

mentally appropriate ways.[82] Visible security measures, such as CCTV cameras and metal detectors situated inside school buildings rather than in outdoor areas, can actually result in heightened disorder and violence and decrease students' and school personnel's perceptions of safety.[83]

The literature on protective security measures for ST sectors beyond just the school sector touches on the potential for unintended consequences. For example, protective measures can convey false senses of security among untrained and unaware employees and patrons, create areas with differentiated levels of risk and security, or displace crime and violence to other, unprotected or less protected spaces.[84]

Finally, the literature identifies very little about the cost-effectiveness of security technologies. Some of the more-economical responses to school shootings in particular have included the implementation of access control measures, such as locking doors, screening visitors, and requiring ID badges.[85] These measures represent lower-cost approaches to promoting security than implementing such technologies as CCTV cameras and than hiring dedicated security personnel. These measures are also unlikely to cause harm or be unacceptable to facility patrons.[86] But their effectiveness in the face of both everyday forms of crime and violence and infrequent high-casualty mass attacks has yet to be subject to rigorous evaluation and remains largely unknown.

Findings from the Literature

Our review of the literature on protective measures for STs shows that there is little robust evidence about the effectiveness of protective measures. Technologies are often selected by schools, houses of worship, and other facilities on an ad hoc basis—at times, in direct response to the fear and anxiety brought on by recent tragic events. The literature and other material that facility personnel can access about the effectiveness of various technologies is often anecdotal in nature, focuses on reducing criminal acts, or presents conflicting results

[82] Bachman, Randolph, and Brown, "Predicting Perceptions of Fear at School and Going to and from School for African American and White Students"; Gastic, "Metal Detectors and Feeling Safe at School"; Huskey and Connell, "Preparation or Provocation?"; Moore-Petinak et al., "Active Shooter Drills in the United States"; Nance, "Student Surveillance, Racial Inequalities, and Implicit Racial Bias"; National Association of School Psychologists, National Association of School Resource Officers, and Safe and Sound Schools, *Best Practice Considerations for Armed Assailant Drills in Schools*; Perumean-Chaney and Sutton, "Students and Perceived School Safety."

[83] Hanover Research, *Best Practices in School Security*; Jackson, Diliberti, et al., *Teachers' Views on School Safety*; Johnson et al., "Surveillance or Safekeeping?"

[84] Cerezo, "CCTV and Crime Displacement"; Coaffee, "Rings of Steel, Rings of Concrete and Rings of Confidence"; Dalgaard-Nielsen, Laisen, and Wandorf, "Visible Counterterrorism Measures in Urban Spaces."

[85] Schwartz et al., *The Role of Technology in Improving K–12 School Safety.*

[86] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; Steiner et al., *Challenges in Implementing Physical Security Measures in K–12 Schools.*

and findings. This is especially true for such materials for the K–12 education sector, which has experienced rising levels of gun violence over the years.[87]

Another complication is that contextual factors affect the effectiveness of measures. Such factors as building occupants' behavior during emergencies, occupants' awareness of how various countermeasures work, and the nature of incidents themselves (insider versus outsider attacks) all affect whether a security technology will provide its intended benefit. These findings signal that training and practice are likely critical to maximizing the security benefits of different security technologies across diverse ST sectors and that there is no one-size-fits-all solution to physical security in ST-CPs.

The implications of our review are manifold. First, system-based approaches to physical security can help mitigate some of the challenges that ST facilities face when planning for physical security improvements. These approaches situate physical security and protective measures as components of a broader approach to safety and security—including activities to prevent threats and recover from traumatic incidents—thereby encouraging planners to take a holistic view. Moreover, system-based approaches emphasize the benefits of planning for layered security, in which the integration of various measures and technologies helps avoid having single points of failure and in which policies and training help reinforce and ensure the security benefits of protective measures. By supplementing technological approaches to security with nontechnological ones, system-based approaches can also help mitigate some of the harmful impacts that technology-heavy approaches can create, such as increased fear or the degradation of the openness and welcoming nature of a school or other location's climate.

Second, providing the necessary information to facility and event employees, volunteers, and patrons is critical to maximizing the security benefits of protective measures. Some measures, such as mass-notification systems, will have little value during an emergency if people are unaware that they exist, are not registered in a system, or do not know what to do if they receive a notification.[88] As a result, emergency preparedness initiatives that focus on training and education for facility employees and volunteers, as well as patrons, could be especially critical to improving response to disasters when they occur.[89] In the K–12 school sector, such organizations as the National Association of SROs and the National Association of School Psychologists have developed best-practice guidance to support education agencies in planning drills in a way that minimizes impacts on student and staff mental and physical well-being, as well as disruptions to teaching and learning.[90]

Finally, reminding members of the public about the need to stay aware and report suspicious activity or suspected threats is critical to preventing mass attacks; indeed, research has

[87] Reidman, "K–12 School Shooting Database."

[88] Fox and Savage, "Mass Murder Goes to College."

[89] Weber, Schulenberg, and Lair, "University Employees' Preparedness for Natural Hazards and Incidents of Mass Violence."

[90] National Association of School Psychologists, National Association of School Resource Officers, and Safe and Sound Schools, *Best Practice Considerations for Armed Assailant Drills in Schools*.

shown that well-publicized and easily accessible reporting resources, such as anonymous tip lines, can help encourage bystander reporting and thereby prevent attacks.[91]

Results of the Quantitative Analysis

Measures Aligned with Attack Prevention

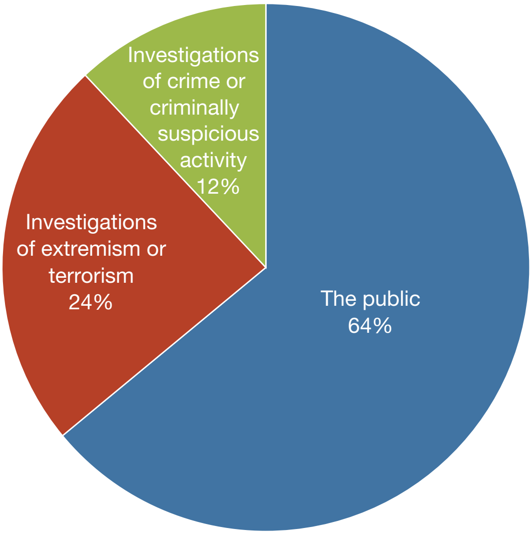
In the MADT dataset, more than half of mass-attack plots (326 of 628) were foiled in advance. Figure 3.1 captures the main sources of initial clues that led to plots being foiled. Importantly, when an initial warning sign was reported, plots were stopped more than 80 percent of the time. In contrast, cases in which initial warning signs were not reported almost always reached execution, by definition.

As shown, tips from the public were responsible for almost two-thirds of initial clues. The public is the first line of defense in preventing terrorist plots. There is, therefore, a critical interest in increasing the number of high-quality tips about potential terrorist plots.

Also of interest were preventions because of discoveries during investigations of terrorism or violent extremism. These were a combination of finding potential attackers because

FIGURE 3.1

Sources of Warning Signs About Attack Plots



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

[91] Moore et al., *A Systems Approach to Physical Security in K–12 Schools*; NTAC, *Averting Targeted School Violence*.

they were new and significant associates of known violent extremists or terrorists (or terrorist organizations); people who wanted to carry out attacks who were new contacts of undercover agents or informants; or suspects found during investigations of lesser terrorist crimes (for example, attacks on property, such as houses of worship, with graffiti marking the attack as a terrorist attack or hate crime).

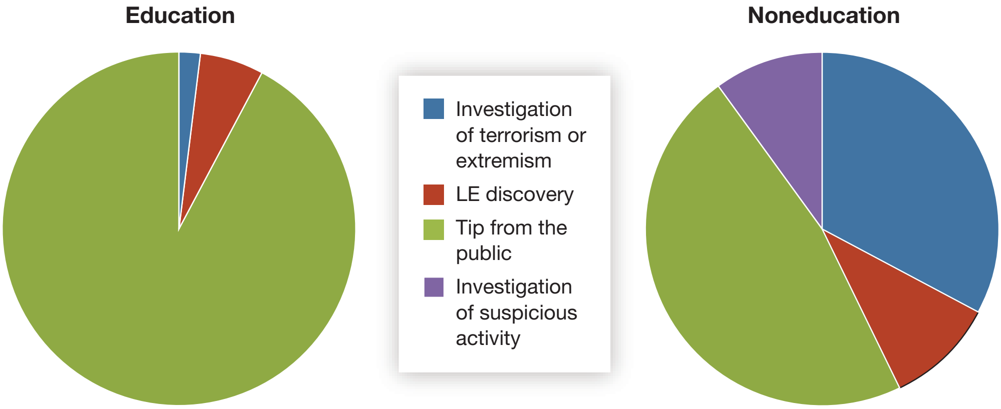
The third major category of initial clues came from discoveries by alert LE. These included investigations of crime initially thought to be ordinary but that ended up being in support of a planned terrorist attack. These clues also included investigations of suspicious activity thought to be potentially related to ordinary crime but found, on further investigation, to be related to a planned mass attack.

Types of initial clues varied with type of attack. Figure 3.2 compares the main sources of initial clues for plots against education facilities with those for all other attacks. Here, the defining characteristic is that the former concerns students who have many colleagues, teachers, and staff who typically are paying attention to each other, whereas the latter usually involve adults, who are generally receiving much less attention. As shown, almost all (more than 90 percent) of prevented plots on education targets are through tips, whereas only about half of other initial clues were through tips.

Figure 3.3 provides more specifics on the initial clues, comparing plots against education targets and plots against other targets.

FIGURE 3.2

Comparing Sources for Initial Clues for Education and Other Sites

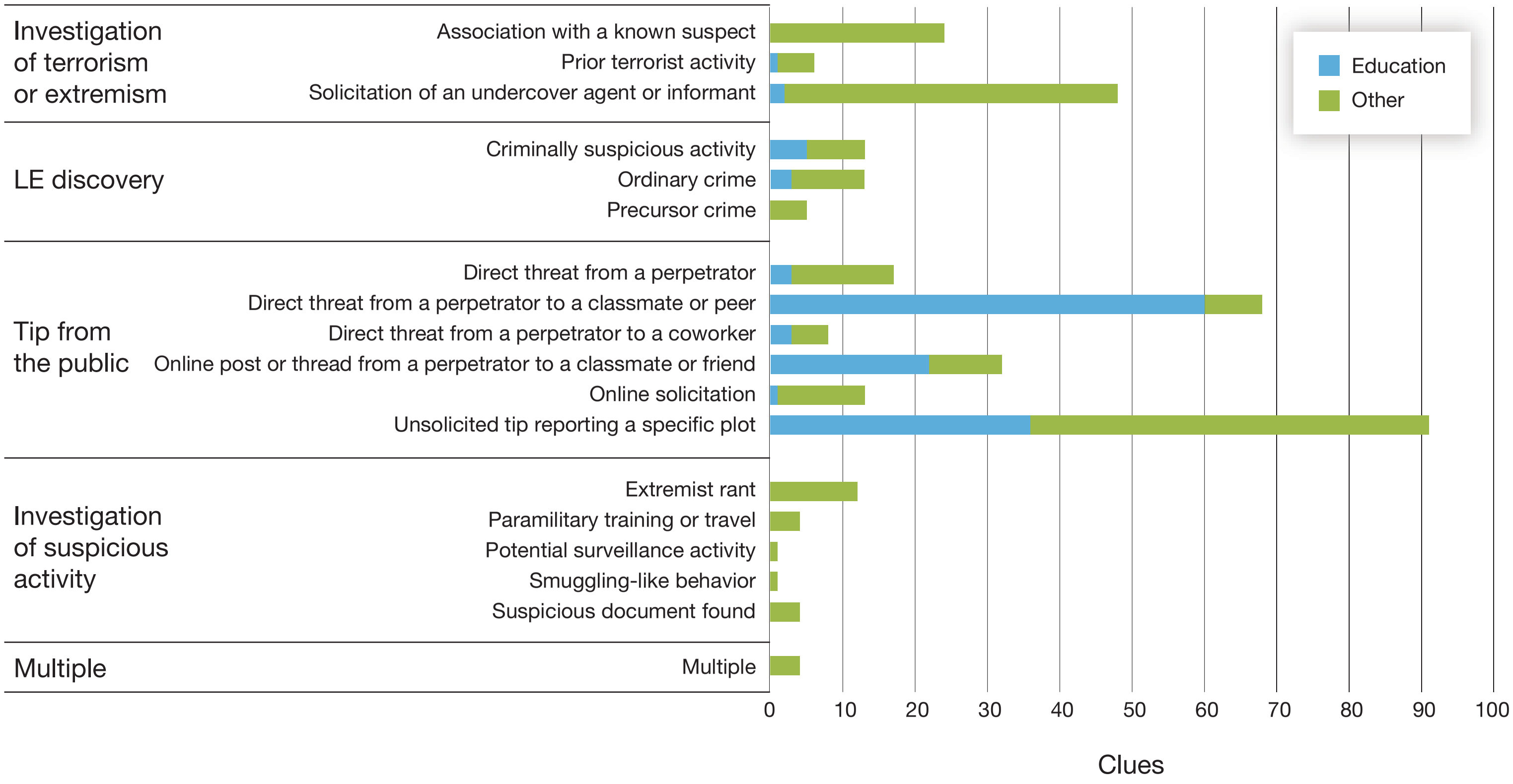


SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated all foiled cases in the dataset (*n* = 326). For purposes of this analysis, *education site* refers to a school, college, or university.

FIGURE 3.3

A Detailed Breakdown of Initial Clues



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

NOTE: The analysis incorporated all failed and foiled cases at education locations (*n* = 136) and noneducation locations (*n* = 228). A precursor crime is a crime preliminary to a large-scale terrorist attack.

Tip from the Public

As noted, tips were, almost exclusively, behind preventing education plots. Types of tips reported include

- a report of a direct threat from a would-be perpetrator to a peer, threatening an attack
- an online post or thread to a classmate or friend leaking information related to plans for an attack
- other details about a specific plot that had been leaked to the reporter.

Tips were also close to half of the initial clues for the noneducation plots (which, as noted, typically involve adults). These included

- online solicitation (an attempt to recruit someone else to join a plot, with at least one of those contacted then contacting authorities)
- a report of a threat from a would-be perpetrator to a coworker
- another detail about a specific plot that had been leaked to the reporter
- self-report (making a direct, detailed, and serious threat to attack to authorities).

The following types of initial clues have substantially increased importance for plots outside of education locations because they apply to adult would-be perpetrators outside of regular monitoring.

Investigation of a Terrorist or Extremist Association

This involves initial clues about a plot discovered because of an ongoing investigation into a past terror attack (usually lesser, such as a property attack), as well as known terrorist and violent extremist organizations. This includes

- a newly discovered and significant association with a known terrorist organization, terrorist, or violent extremist. These are typically found through ongoing investigations (LE and national security) of these organizations and individuals. Importantly, these are significant associations in which the person is making contact in support of carrying out a violent attack; they do not include casual business or other contacts.
- solicitation of an undercover officer or informant during which the solicitor makes clear their desire to participate in an attack
- investigations of prior terrorist activity, such as investigations seeking the perpetrators of lesser terrorist attacks.

Suspicious Activity

Suspicious activity does not provide specific details of a threatened plot but nonetheless is genuinely threatening and has a nexus with mass attacks. Examples have included

- extremist rants that implicitly but seriously threatened violence
- attempts to obtain paramilitary training or traveling to meet up with terrorist or extremist organizations to seek such training
- potential surveillance and probing activity at prospective target sites
- suspicious documents.

Law Enforcement Discovery

This is a clue discovered as part of what initially appeared to be a routine criminal investigation. This includes investigations of (1) crimes that initially appeared to be ordinary and (2) criminally suspicious activity. During these investigations, officers found additional evidence (or received statements) that the crimes were carried out in support of planned terrorist activity.

Beyond a quantitative analysis of initial clues, the MADT includes an extensive treatment of mass-attack plot prevention, including warning signs, recommended organizational structures, recommended processes, and additional educational and implementation resources.[92]

Measures Aligned with Attack Protection

As part of National Institute of Justice (NIJ)–sponsored research for the MADT, we characterized the highest-fatality attacks as occurring at one (or sometimes both) of two canonical types of high-risk venues: a constrained box or a constrained labyrinth. Some sites had similarities to both. Figure 3.4 shows abstract diagrams of these two types of high-fatality venues.

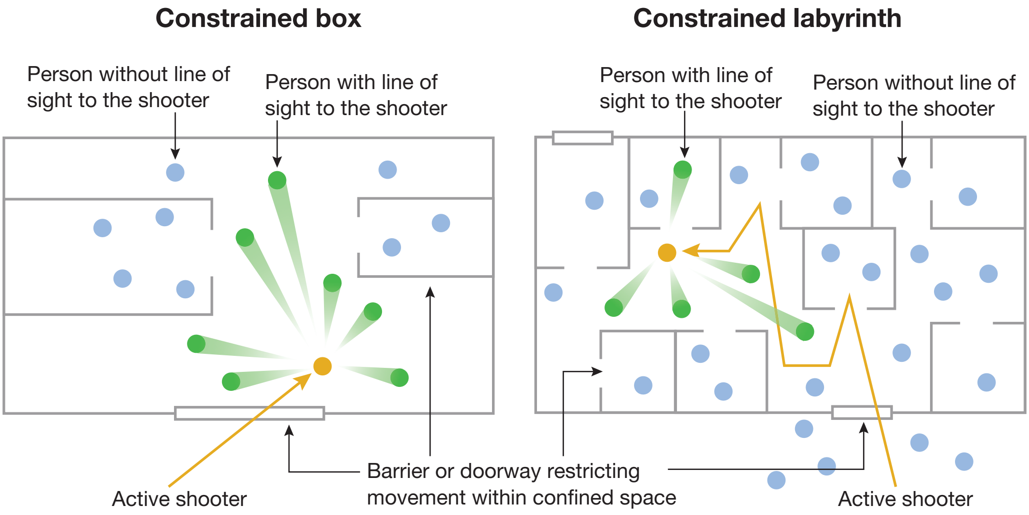
The core characteristic of both types is that someone was able to surprise and attack at close range a crowd of people who had limited ability to escape. The principal difference was one of time—in the constrained box, the shooter surprised and attacked most bystanders at once, whereas, in the constrained labyrinth, the shooter surprised and attacked a smaller group of bystanders over time after moving from room to room.

We conducted a qualitative analysis of a sample of plots with only one or two fatalities to identify factors that seemed to help explain why so few people were killed. We reviewed available information in publicly available media as to how low-fatality attacks in the MADT unfolded, and we identified a set of core characteristics. As shown in Figure 3.5, some of these were factors that are directly under the control of the shooter. However, others were directly related to factors that were either directly or at least somewhat due to site characteristics.

[92] Hollywood et al., *Mass Attacks Defense Toolkit*.

FIGURE 3.4

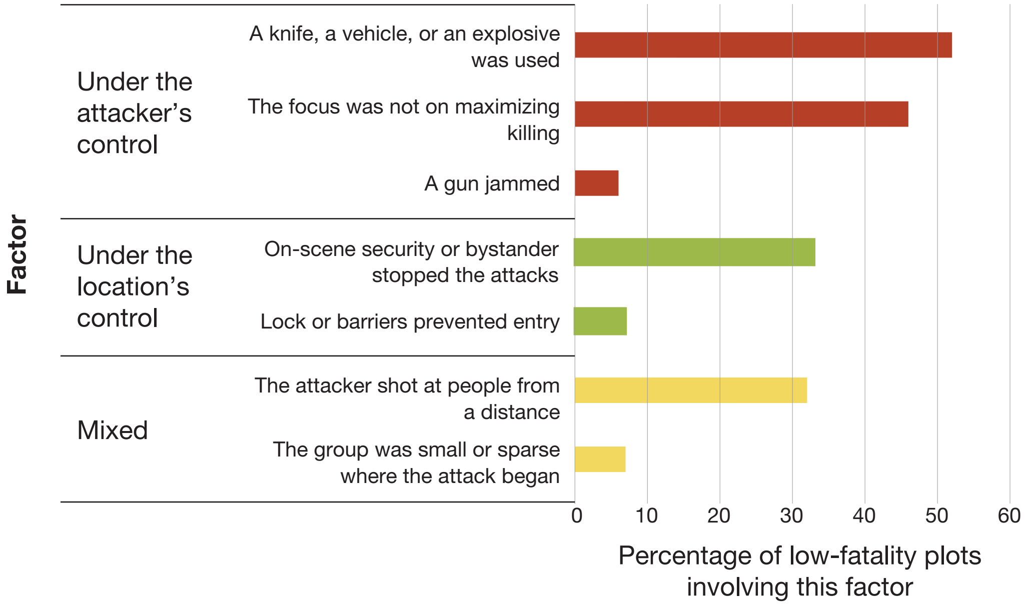
Typical Layouts of Locations of High-Fatality Attacks on Soft Targets and Crowded Places


Constrained box
Constrained labyrinth
Person without line of sight to the shooter
Person with line of sight to the shooter
Person with line of sight to the shooter
Person without line of sight to the shooter
Active shooter
Barrier or doorway restricting movement within confined space
Active shooter

SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

FIGURE 3.5

Factors Associated with Low-Fatality Plots



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.

Factors Under the Attacker's Control

For low-fatality attacks, we identified three major characteristics under the attacker's control. The first was committing an attack other than a shooting; using a knife, a vehicle to ram victims, or an attempted bombing typically had a much lower fatality count. The second was a focus other than maximizing killings; in these plots, shooters shot a few people and left the scene or, in a few cases, decided to just stop shooting. The third was their gun jamming, forcing them to stop shooting.

Factors Under the Location's Control

The first of two major characteristics was the use of locks or barriers that effectively prevented a would-be shooter from getting through critical doors and thus reaching a large crowd. These included both exterior doors (e.g., secured vestibules with multiple doorways required to enter a crowded building) and interior doors (e.g., locked classroom doors that stopped a shooter from entering a full classroom). The second was the behavior of on-scene security or bystanders—they engaged and stopped the attacker. (We discuss bystander or security interventions under "Mixed Factors," next.)

Mixed Factors

There were two characteristics that could be under the control of the shooter or under the attacker. The first was that the attacker shot at people from a distance—in some cases, from outside the targeted building, attempting to fire through windows. In general, the farther away a shooter is from their intended targets, the less likely they are to hit them; the distance also gives bystanders much more freedom to move away from attackers. In some cases, this appears to have been at least partly deliberate, for whatever personal motivation. In other cases, locks, secured walk-up areas, or other barriers appear to have driven shooters to start firing from a highly disadvantageous position and distance.

The second characteristic was that the shooter initially fired on a small or sparse group of people when the attack began, which gave most others warning and hence time to escape or secure themselves and gave LE more time for an armed response. This appeared to have been a mix of matters of choice and shooters being deterred by secured entries or passageways and thus starting to open fire from where they could.

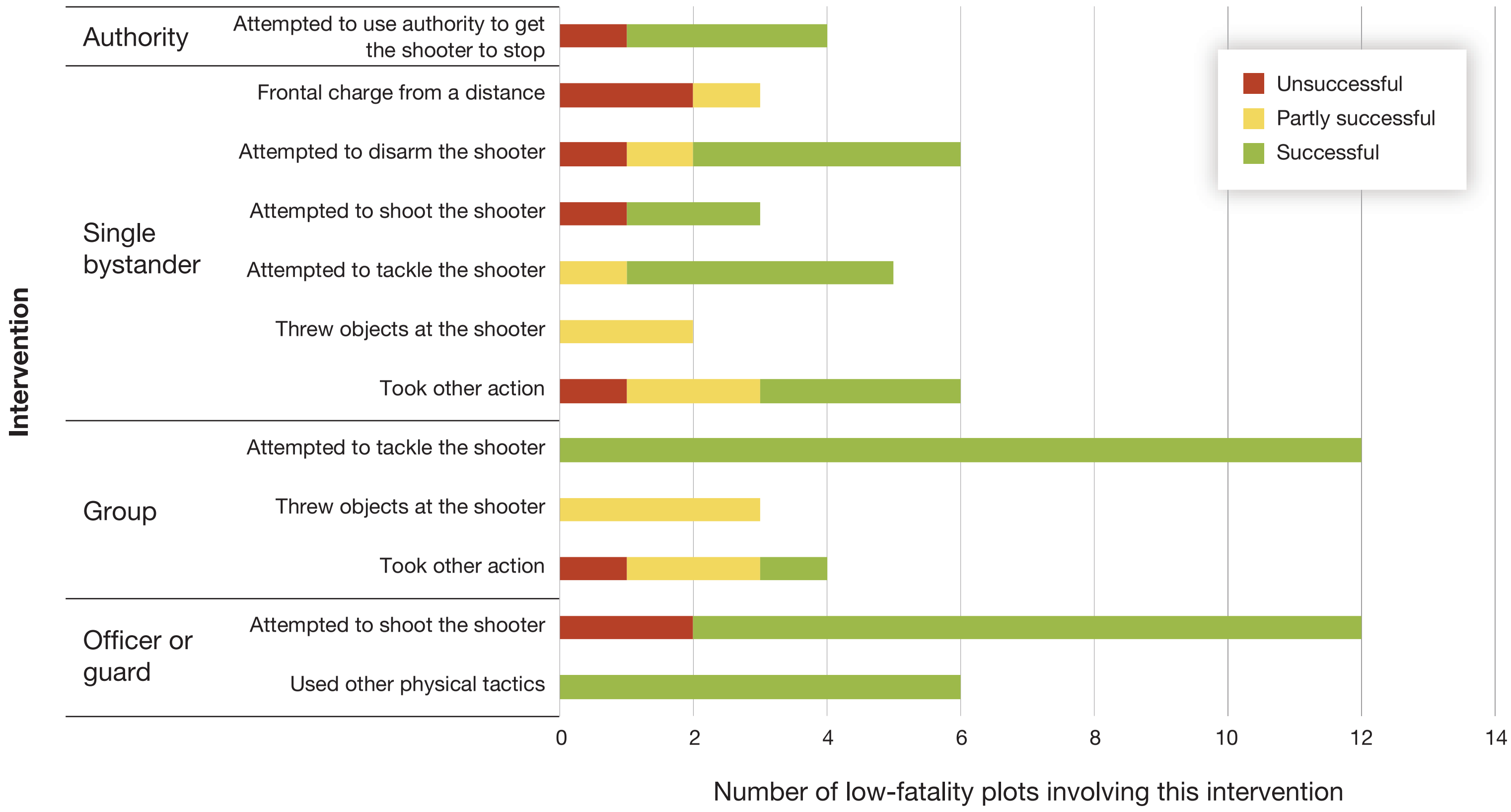
Bystander and On-Scene Response

Figure 3.6 shows the major types of interventions that bystanders employed against mass shooters, as well as the results. Here, *unsuccessful* means that a bystander did not stop the shooting. *Partly successful* means that a bystander got the shooter to pause and flee a room or other specific area. *Successful* means that a bystander halted the shooter from any subsequent firing (and casualties). The figure captures interventions from four types of bystanders:

- authority figures to shooters, typically at schools (e.g., principals, teachers)
- single civilian bystanders (i.e., not professional police or security)

FIGURE 3.6

Interventions Against Shooters and Their Results



SOURCE: Derived from data in Hollywood et al., *Mass Attacks Defense Toolkit*.
NOTE: The analysis incorporated any completed case in the dataset that had fewer than two fatalities (n = 103).

- groups of civilian bystanders
- on-scene armed officers or security guards.

Overall, the data make clear that, **if bystanders are confronted directly with a shooter, they should immediately attempt to tackle and disarm the shooter**. This was the most frequently used and consistently effective intervention. Group tackling successfully stopped shootings in all of the dozen times it was used; individuals were always at least partly successful, and they were fully successful in four of five attempts.

Armed responses by guards, on-scene officers (typically off-duty), and, occasionally (in three cases), civilian bystanders were often effective at stopping shooters. However, they were sometimes ineffective: in cases in which the armed responder could not engage (could not reach the shooter for whatever reason), failed to engage, or the shooter shot the armed responder first.

Throwing objects was consistently successful at getting a shooter to pause and leave, albeit not to stop the shooting itself.

Other tactics by civilian bystanders—directly disarming by attempting to grab arms and using other physical tactics (which covered a wide variety of efforts, including clubbing the shooter, pushing the shooter out of a room, driving into the shooter, chasing the shooter, and brandishing a weapon) also showed some success, albeit not as much as tackling. Similarly, other nonshooting tactics by on-scene security and officers, including tackling, tasering, and otherwise engaging shooters, were also consistently successful.

In four cases in the MADT dataset, authority figures in schools attempted to order shooters to stop shooting; they were successful in three. (In the one case of a bystander attempting to talk down a shooter, they were unsuccessful.)

A Case Study Analysis

An Overview of the Case Studies and Our Approach to the Analysis

As discussed in Chapter 2, we selected six mass attacks that occurred between 2013 and 2021 as case studies for further analysis. The goal of the case studies was to identify factors that influenced the outcome of each incident in terms of casualty levels. For each case, we considered aspects related to the incident location (e.g., facility type and site configuration), the weapon used, the attacker's movement during the attack, any protective measures in place at the facility at the time of the incident, and how these protective measures worked or failed to work in terms of mitigating casualties. Table 3.2 summarizes each of the six case studies included in our analysis.

Case Study Findings

In our analysis of each case, we sought to highlight the role that protective measures might have played in the incident's eventual outcome to better understand the potential effective-

TABLE 3.2

Overview of Case Studies Selected for Analysis

Case Study	Date	Description
Manchester Arena bombing[a]	May 22, 2017	A suicide bomber detonated a homemade bomb filled with shrapnel in Manchester Arena's open-access main foyer as concertgoers were leaving an Ariana Grande concert in Manchester, England. Twenty-three people were killed in the incident, and more than 1,000 others were injured.
Pulse nightclub shooting	June 12, 2016	A gunman entered the Pulse nightclub in Orlando, Florida, with an AR-15 rifle and a Glock 9-mm handgun and fired at patrons, killing 49 people and injuring 53. The gunman continually shot as he traveled through the club, including on the dance floor and in bar areas, before barricading himself in a restroom, where he continued to shoot patrons. Police eventually penetrated the building and killed the attacker.
MSDHS shooting	February 14, 2018	A former student at MSDHS in in Parkland, Florida, entered campus through an unlocked gate carrying an AR-15 semiautomatic firearm. He made his way across campus and entered a three-story building containing classrooms, where he killed 17 people (14 students and three staff members) and wounded 17 others. The gunman then discarded his weapon and blended in with crowds evacuating the school to leave the campus. He was later arrested later by police.
El Paso, Texas, Walmart shooting	August 3, 2019	After casing a Walmart store in El Paso, Texas, a gunman retrieved a GP WASR 10 from his vehicle and shot customers in the parking lot and inside the store. He killed 23 people on site and injured 23 others. Prior to the attack, the gunman had posted a manifesto citing as inspiration white nationalist ideologies and the Christchurch, New Zealand, mosque shootings that had occurred 141 days prior. He was arrested shortly after fleeing the scene and subsequently pled guilty to federal hate crimes.
Arapahoe High School shooting	December 13, 2013	A student entered Arapahoe High School in Centennial, Colorado, through an unlocked door near a main hallway. Armed with a pump-action shotgun, large hunting knife, and three Molotov cocktails, the shooter fired into the hallway, killing one student, and moved into the library to locate a teacher who was his likely intended target. The teacher was able to flee, and the gunman died in the library of a self-inflected gunshot wound.
Waukesha, Wisconsin, Christmas parade attack	November 21, 2021	An attacker drove a sport-utility vehicle through police barricades and into a crowd of spectators and participants along a parade route in Waukesha, Wisconsin. Six people were killed in the attack, and 62 were injured. To escape the scene, the attacker crashed his vehicle through additional barriers near the end of the parade route. He was arrested by police soon thereafter.

NOTE: GP = general purpose; WASR = Wassenaar Arrangement semiautomatic rifle.

[a] This case is not in the MADT dataset because it occurred outside the United States. We included it because it permitted us to examine a recent significant bombing attack on a major event venue.

ness of measures in protecting diverse types of ST-CPs. Our review of publicly accessible accounts of each case, including police and emergency responder AARs, commission reports, and news stories, helped us identify the impact that seven types of protective measures had on incident outcomes. Table 3.3 provides an overview of our assessment.

In the rest of this section, we elaborate on several critical takeaways and lessons learned about how security measures worked and could be improved at the ST-CPs included in our case studies and across these sectors more broadly. We focus on four specific areas: perimeter security, CCTV technology, security personnel, and training and awareness.

Perimeter Security

The importance of policies on keeping a facility's exterior doors closed and locked was a key takeaway from our case study analyses. The incident at MSDHS demonstrated multiple shortcomings in this area; although the campus's outer perimeter included designated entryways for pedestrians, several of these gates were opened approximately 25 minutes prior to the end of the school day on the day of the incident, and none was staffed by security or other personnel.[93] In the case of Arapahoe High School, the shooter entered a school building through an unlocked door that, according to school policies, should have been locked.[94] Had both of these schools maintained a higher level of security at their outer perimeter and building perimeter layers—by, for example, regularly securing gates and exterior doors and adding staff presence at various entry points—the attackers might have been deterred or detected and stopped. Indeed, an alert school staff member in the parking lot of Arapahoe High School on the day of the shooting helped alert staff inside the building—including dedicated security staff—of an emergency.[95] A locked exterior door could have greatly improved the chances of thwarting the attack altogether.

The ability to quickly lock doors is another critical security feature that was absent across several cases—most notably, the El Paso Walmart shooting, in which employees did not appear to have the capability to automatically lock the facility's doors following notification of an active-assailant emergency, and during the shooting at MSDHS, during which teachers were unable to lock their classroom doors from the inside.[96] By contrast, classroom doors at Arapahoe High School were equipped with lockdown magnets, which help to speed the door-locking process in the event of a school lockdown.[97]

[93] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President*, p. 41.

[94] Dorn et al., *Post-Incident Review*, p. 29.

[95] McCauley, *Investigative Report*.

[96] Conley, "Why the El Paso Massacre Was a Security Failure"; MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives, and Senate President*, p. 45.

[97] Dorn et al., *Post-Incident Review*, p. 46. These magnets, however, did not play a role in mitigating casualties during the incident because the shooter did not make any attempts to enter classrooms on the day of the incident.

TABLE 3.3

The Role of Security Measures in the Case Studies

Case	LE	Non-LE Security	Barrier	Door System or Entry Screening	CCTV or Other Surveillance	Communication Technology	Employee Training
Manchester Arena bombing	–	–		+	–	–	–
Pulse nightclub shooting	–						
MSDHS shooting	–	–		–	–	–	–
El Paso, Texas, Walmart shooting		–		–	–	+	+
Arapahoe High School shooting	+	+		–	–	+	
Waukesha, Wisconsin, Christmas parade attack	–		–				

NOTE: + = the security measure worked to limit the number of casualties; – = the security measure constituted a point of failure during the incident, potentially leading to increased casualties; and a blank cell indicates that the measure played no discernible role in the incident's outcome.

Another important takeaway relates to ensuring that a facility's outermost perimeter extends enough to provide sufficient space for screening, dispersion, and the implementation and use of other protective measures. The Manchester Arena bombing, for example, occurred in the City Room, an area that remained open to the public and into which concertgoers exited at the concert's end; concertgoers were subject to screening procedures only when entering the arena itself.[98] Although the bomber did attract some suspicion, he was allowed to enter and move about the City Room prior to and during the concert without being screened.[99] Extending certain screening measures—such as random bag checks—into this area could have deterred the bomber or helped further identify his behavior as suspicious prior to the attack. Notably, extending an outer security perimeter is often insufficient to prevent an attack and might only displace harm to another unmonitored or uncontrolled area. Nevertheless, the implementation of additional screening measures for the City Room on the day of the incident could have forced the bomber to denotate his device in a different, less densely packed area, thereby lessening the number or severity of casualties.

Pulse nightclub, targeted by an active shooter in 2016, also lacked perimeter security at the time of the incident. The club had no screening measures or procedures, such as pat-downs or bag checks, in place at the entrance. These measures could have deterred the shooter altogether or detected a weapon as he attempted to enter the nightclub.

Finally, the vehicle-ramming incident in Waukesha, Wisconsin, demonstrates the importance of perimeter security for outdoor events: The strategic placement of resilient barriers clearly designating outer boundaries throughout an event can help to prevent or slow vehicle-borne and other types of attacks.[100]

Closed-Circuit Television Technology

Our case studies identified several instances in which CCTV camera technology played critical roles in affecting incident outcomes. Specifically, we assessed that the lack of live monitoring of CCTV video feeds led to failures in mitigating casualties in at least three cases; cameras in place at various targeted locations captured the attacker's movements prior to or during the attacks, but the footage was not actively and consistently monitored by security staff, thereby severely limiting the security benefits provided by the technology. In the case of the Manchester Arena bombing, for instance, CCTV camera footage was only inconsistently monitored on the day of the incident, and the security company hired to help provide security and monitor the control room did not have the appropriate licensing and training

[98] Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, p. 29.

[99] Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, pp. 23–24.

[100] Lemoine, "Waukesha Memorial Day Parade Returns."

to perform its tasks.[101] Moreover, security staff assigned to the control room during the concert were absent around the time of the bombing. Had they been at their assigned posts and appropriately trained and certified to identify suspicious activity, they might have flagged the bomber's presence prior to the detonation. CCTV cameras were also a point of failure during the shooting at MSDHS: Security staff were not actively monitoring camera footage at the time of the incident and not properly trained on how to operate the school's camera system. The MSDHS Public Safety Commission concluded that "this lack of familiarity and training adversely affected law enforcement response."[102] Evidence also suggests that security staff were not monitoring CCTV footage during the Walmart shooting in El Paso or the shooting at Arapahoe High School.[103] Together, these cases demonstrate the importance that providing security staff the ability to monitor live CCTV camera feed could have for incident outcomes, largely by increasing the probability of early detection.

The incidents in our case study analysis also highlight the need for regular maintenance checks on technology, such as CCTV cameras. In the case of the MSDHS shooting, first responders were initially confused about whether the CCTV footage they were viewing was live; although campus security personnel relayed information to LE stating that the CCTV footage was relaying live images, the footage was, in fact, delayed by approximately 26 minutes and hampered first responders' ability to accurately respond to the shooter's movements in real time.[104] In the case of the Arapahoe High School incident, security personnel later reported that the camera system in place was "out of date" and poorly maintained and that different cameras were associated with different time stamps.[105] Although, in this latter case, these flaws had no discernible impact on the incident's eventual outcome, the MSDHS shooting demonstrates the negative implications such issues can have on effective response to active-shooter incidents.

Finally, the Manchester Arena bombing demonstrates the importance of ensuring that CCTV cameras cover as much of a facility as possible and do not create so-called blind spots. A postattack inquiry launched by the United Kingdom government identified a CCTV blind spot in the area where the attack took place of which security staff were not aware. The bomber, himself aware of this blind spot, spent a notable amount of time in this area prior to the bombing, eventually attracting the suspicion of at least one member of the pub-

[101] Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, pp. 117, 130.

[102] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives, and Senate President*, p. 47.

[103] Conley, "Why the El Paso Massacre Was a Security Failure."

[104] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives, and Senate President*, pp. 35–37.

[105] McCauley, *Investigative Report*, p. 32; Dorn et al., *Post-Incident Review*, p. 38.

lic.[106] According to the inquiry, "had the area been covered by CCTV . . . it is likely that this behavior by [the bomber] would have been identified as suspicious by anyone monitoring the CCTV."[107]

Security Personnel

Security personnel played a key role in influencing the outcomes of nearly every case included in our analysis. Most notably, our case studies demonstrate the importance of ensuring that security personnel have regular and facility-appropriate training, including active-shooter and terrorism awareness training. In the case of the shooting at MSDHS, school staff had received only one training on active-assailant response procedures shortly before the shooting.[108] Moreover, the school did not have an established active-assailant response policy at the time of the shooting, nor did it have any written or trained-on policies on code red or lockdown procedures.[109] Had employees—school staff and security personnel alike—received more-thorough and regular active-assailant training prior to the incident, including training on lockdown procedures, the incident's outcome might have been different. Specifically, campus security staff could have implemented a lockdown or other response action immediately upon noticing the shooter make his way into and across campus, prompting teachers and other school staff to take specific actions inside school buildings, such as closing and locking classroom doors and moving students to safe corners.

In the case of the Manchester Arena bombing, further training for both facility security staff and police officers on hostile reconnaissance and counterterrorism awareness might also have helped prevent the attack altogether or at least change the outcome. Security staff and LE personnel present at the arena on the day of the incident, including those stationed throughout the City Room, failed to identify the bomber's presence as suspicious and did not respond with a sufficient sense of urgency when members of the public notified them of his potentially suspicious presence.

Our cases also demonstrate the potential deterrent effect of uniformed security personnel at a facility's outer perimeter layer. In the case of the Pulse nightclub shooting, no security was present at the club's entrance. An off-duty police detective providing security was stationed in his vehicle in the club's parking lot area when the shooter entered, but he did not notice anything suspicious and alerted additional officers only after hearing gunshots

[106] Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, pp. 23–24.

[107] Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, p. 17.

[108] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives, and Senate President*, p. 50.

[109] MSDHS Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives, and Senate President*, p. 49.

coming from inside.[110] Had the facility maintained a greater security or LE presence around its exterior, these measures might have worked to deter the attacker from selecting this club as his target. Security at the entrance might also have stopped or slowed the attacker. Indeed, prior to arriving at Pulse, the shooter drove to another club that appeared to have substantial door security, including pat-downs and substantial police presence. He continued to search for nightclubs in the area and eventually settled on Pulse, though it is unclear whether the level of security at the first club served as a deterrent.[111]

Uniformed security personnel were not present during the attack on the El Paso Walmart facility in 2019.[112] The presence of armed or unarmed security guards outside the store might have stopped the incident sooner or deterred the shooter from targeting the specific location in the first place. However, the presence of uniformed security and LE personnel did not effectively deter or limit casualties in other cases, including the MSDHS shooting and Manchester Arena bombing. These failures highlight the importance of providing security personnel with regular and appropriate facility- and threat-specific training.

Training and Awareness

Training and awareness around active-shooter events and other types of mass violence is also important for facility employees, volunteers, patrons, and members of the public; in the event of an incident, each can play a role in safeguarding a facility. In some of our cases, more-regular active-assailant training for nonsecurity personnel, including training on lockdown procedures, could have better prepared facility staff to respond during an active incident. This was the case during the MSDHS shooting, in which training and drills prior to the incident could have increased school staff members' awareness of and familiarity with specific lockdown procedures. Indeed, the value of such training is perhaps best exemplified in the context of the El Paso Walmart shooting, in which the store manager alerted other employees about the incident over his radio and an employee at an inlet inside the Walmart locked themselves and customers in a back room until police arrived.[113] Other Walmart employees ushered customers into steel shipping containers located in the back of the store.[114] These actions effectively helped to reduce the number of casualties during this attack.

Our cases suggest that there are various ways to increase general awareness about the value of such procedures across different STs. Facilities can consider posting reminders about

[110] Doornbos et al., "New Pulse Review from Orlando Police Reveals Details, Lessons Learned"; Hennessy-Fiske, Jarvie, and Wilber, "Orlando Gunman Had Used Gay Dating App and Visited LGBT Nightclub on Other Occasions, Witnesses Say."

[111] Salman, motion to preclude improper argument in government's opening statement.

[112] Chavez, "A Family Wounded in the El Paso Massacre Is Suing Walmart over Lack of Security."

[113] Basner, "If You Hear a 'Code Brown' While Shopping, Get Out of the Store Immediately"; Garrison et al., "At Least 20 Dead, 26 Wounded, Lone Suspect in Custody After Rampage at El Paso Walmart."

[114] Garrison et al., "At Least 20 Dead, 26 Wounded, Lone Suspect in Custody After Rampage at El Paso Walmart"; Mosbergen, "Walmart Employee Helped More Than 100 People Escape El Paso Shooting."

key safety practices and about staying vigilant for threats and what to do if staff notice potentially threatening behavior. Reminders can outline specific steps to take in the event of a violent incident, methods for contacting security personnel, and the importance of reporting suspicious or unusual behavior more generally (e.g., "see something, say something"). Such measures are relatively low-cost and can help prevent and mitigate possible incidents.

Insights on Preventive and Protective Measures from Subject-Matter Experts

We spoke with multiple security industry and LE professionals about a variety of ST-CP topics, including coordination and response to incidents, assessments and training, threat, and trends in technology. Their insights helped formulate the landscape assessment and identified gaps in ST-CP security that warrant further examination.

Coordination and Response

The main theme to emerge from discussions on coordination and response to ST-CP incidents is the need for cross-agency coordination and communication during an incident. The responses to several incidents have suffered because of a lack of coordination and ability to communicate between agencies. In addition, sites should have procedures in place to contact LE when an incident occurs, and there should be clear lines of authority if multiple agencies are responding. Communication methods should be improved by investing in technology that allows multiple people to communicate at the same time, such as video teleconferences. Blue force–tracker technology that allows first responders to know the position of all friendly forces in real time and has video-teleconferencing capability is an emerging solution to the problem of coordination and has been successfully tested during training events.

Training and Assessments

Training and site security assessment were identified as key elements to provide effective security to ST-CP sites. Site assessments are provided by both U.S. government entities and private companies. CISA, through the Protective Security Advisor program, provides on-site assessments to identify security gaps. USSS also provides resources on training, educational materials, and security doctrine. Private security companies can provide on-site assessments and work with security system integrators to determine the best solution to a site's specific security requirements.[115] As discussed later in this chapter, the main problem in performing assessments is the lack of knowledge that site operators have about the resources available.

[115] Security industry SMEs, interview with the authors, April 19, 2023.

On training, several requirements were emphasized. First was the need to incorporate medical personnel into warm zones around an incident.[116] Training is too often provided strictly to tactical teams tasked with entering a venue. There is a need for cross-disciplinary teams of responders who can stop shooters and respond to medical needs at the same time. There is also a need for repeat training to ensure that personnel can exercise muscle memory in an unfamiliar location. There is a noted difference between responders who have attended only one training class and those who have trained regularly and across jurisdictions.[117]

Trends in Security Technology

Trends in protective measures center on traditional security measures, such as cameras, fencing, lighting, early warning sensors, and secure vestibules and entry systems. New technology, however, is beginning to be used that has the potential to detect possible threats earlier and help first responders as an incident is unfolding. These include video analytics, virtual fencing, and virtual floor plans. Such technologies as metal detectors can detect weapons only while in the entrances of a building, often in a crowd, giving the attacker the chance to initiate an attack even if detected. The goal should be to move the possible point of detection of weapons or suspicious behavior as far from the venue as possible.[118]

AI was often mentioned among technology trends in security. This term, however, has different meanings across the industry. One type of AI mentioned as having the potential to increase detection and assist in improving response was video analytics. Cameras are now available that incorporate video analytics, with the ability to detect suspicious behavior, such as wearing clothes not appropriate for the weather or possible hidden weapons, including firearms and baseball bats.[119] AI can also be incorporated in virtual fencing, in which cameras with analytic capabilities cover areas that lack physical fencing. AI can send alerts to security personnel when suspicious activity is detected, allowing more-comprehensive situational awareness for resource-limited sites where security might have responsibility for both monitoring cameras and physically patrolling an area.

Virtual floor plans are another emerging technology that could assist first responders. Some event locations are putting their floor plans online, which would allow first responders to review critical site information before arriving at and entering the site. This can be accomplished with mobile applications dedicated to accessing floor plans, so a first responder has access on their phone or other mobile device.[120]

[116] *Warm zone* refers to a location that is believed to be secure from any further shooting (or other attacks and attackers) but has not been officially cleared, rendered safe, and reported as such by LE.

[117] LE SMEs, interview with the authors, May 19, 2023.

[118] Security industry risk management SMEs, interview with the authors, June 2, 2023.

[119] Security industry risk management SMEs, interview with the authors, June 2, 2023.

[120] Security industry risk management SMEs, interview with the authors, June 2, 2023.

Unintended Consequences of Measures

Protective measures are designed to make venues safer but also can have unintended consequences that diminish their value or create additional problems. The two main unintended consequences that were apparent from the SME interviews were (1) creation of an intimidating atmosphere at a venue and (2) an increase in security at one area of a venue but a decrease in security at other areas. The cost of security measures and how those costs affect venue budgets were also considerations.

Security measures, such as security vestibules, bag checks, and metal detectors, can create an intimidating environment in which employees or patrons can feel unsafe. This is an especially important consideration for K–12 schools. As one security industry professional put it, "[We] don't want schools looking like prisons."[121] Large venues, such as sports arenas, can incorporate these measures more easily than smaller ones can because it is more culturally accepted, but smaller venues that want to maintain an inviting atmosphere might forgo them for the sake of creating a more welcoming environment, thereby allowing an attacker to gain entrance with a weapon more easily.[122]

These types of security measures also tend to create long lines as people try to enter a venue. The area is often outside a security perimeter and can become clogged with a large number of people, making it an inviting target. Security measures—such as walk-through scanners equipped with technology (e.g., millimeter wave radar)—that can identify weapons and move people efficiently through entry-controlled areas can help create a more welcoming atmosphere and decrease perceptions of hostility in an environment.[123]

Robust and observable security measures can also have the unintended consequence of altering an attacker's target selection. A would-be attacker's surveillance of a target could identify difficulties in accessing the target and carrying out a planned attack. This could cause the attacker to change to a softer target that has less security.[124] Also, increased spending on security can negatively affect a venue's budget. This is especially true for smaller venues and municipalities.

Gaps and Shortfalls

Interviewees identified several gaps in which additional investments in resources or information might improve overall ST-CP planning and response. First, they said that grant funding has been too focused on developing and deploying physical barriers and surveillance at the expense of planning for and responding to an attack. Additional resources should be focused, they said, on integrating LE into responding to suspicious behavior to intercept a

[121] Security industry risk management SMEs, interview with the authors, June 2, 2023.

[122] Event venue security personnel, interview with the authors, July 20, 2023.

[123] Security industry risk management SME, interview with the authors, June 2, 2023.

[124] LE SME, interview with the authors, May 19, 2023.

threat before an attack and for responding to an attack as it is taking place.[125] Additionally, communication planning, including exercises to deconflict communication channels during an attack, is key to response, they noted. Interviewees indicated that the responses in many incidents suffered from communications failing at critical points, with radios not functioning in certain environments or radio channels becoming saturated with too much use.[126] They said that additional ST-CP physical areas would benefit from expanded resources and attention. Many rural areas have older buildings, such as schools, that do not have modern protective measures and would be expensive to upgrade. Additionally, interviewees noted, the dispersed nature of possible ST-CP sites in rural areas means longer response times.[127] Additional resources to upgrade facilities and improve response in these areas would be beneficial. Likewise, soft areas outside hardened targets, such as the public areas of an airport before security screening, have not received enough attention and still present attractive targets.[128]

The grant application process was one area in which multiple experts expressed frustration. Many small-venue security managers said that they did not know where to go to find information on what grants were available and how to apply. Larger venues can have personnel dedicated to grant-writing, but smaller organizations do not typically have personnel who are well-versed in this process.[129] Likewise, local officials might not have expertise in grant-writing, so they cannot answer questions posed by the venues. Questions can be raised to the state or federal level, but this takes more time and resources. Also, there is no feedback on why a grant application was rejected, so mistakes cannot be fixed for the subsequent iteration.[130] Because of budget restrictions, grants are a critical source of funding to accomplish major improvements, causing an important process to often lack the resources and information necessary to exploit it.[131]

Like the lack of information on grant accessibilities and processes, one last gap identified in the interviews was the lack of knowledge about where to get information on ST-CP prevention and assistance in determining the needed level of protection. This would include risk assessments for individual sites. Although government organizations, such as CISA, provide advice and evaluation for a site in this regard, many site managers do not know that the resource exists. Additional public outreach could help site managers connect with the resources available and improve site security.[132]

[125] LE SMEs, interview with the authors, May 19, 2023.

[126] Security industry SMEs, interview with the authors, April 19, 2023.

[127] Security industry SMEs, interview with the authors, April 19, 2023.

[128] LE SMEs, interview with the authors, April 3, 2023.

[129] National-level, religious nonprofit community relations council personnel, interview with the authors, July 19, 2023.

[130] Local-level emergency management agency personnel, interview with the authors, July 28, 2023.

[131] Event venue security personnel, interview with the authors, July 20, 2023.

[132] LE SMEs, interview with the authors, April 3, 2023.

Summary of Findings on Preventive and Protective Measures

The literature review, attack data, case studies, and interviews with security SMEs provided a great deal of information on the current state of preventive and protective measures and future trends. A summary of the key findings is provided in this section.

Threat Characterization

The typical threat actor has evolved from an al Qaeda–type terrorist to a more non-ideological, grievance-based actor. Most ST-CP attacks are now committed by individuals with grievances against specific individuals or groups.

The internet has given threat actors expanded resources and exposure. The internet gives a threat actor an expanded ability to conduct extensive reconnaissance and choose targets. Internet research combined with physical surveillance can provide a detailed target profile and allow an attacker to maximize the effects of an attack. The internet also allows increased exposure of the attacker, enabling the spreading of manifestos and justifications. An attack can be live streamed to increase the attacker's fame and exposure.

Prevention

Tips from the public are important to foil attacks. Terrorism investigations and reports on criminally suspicious activity are important, but 64 percent of foiled attack plots were stopped because of public tips.

Site Protection Technology

Little information exists on the effectiveness of preventive and protective measures. Although a great deal of information is available on the types of measures employed at sites, little has been done to assess their effectiveness in preventing or stopping attacks. Security measures are often implemented ad hoc. Contextual factors also greatly affect effectiveness.

Technology can play an important role in preventing and stopping attacks but must be used properly. Security measures, such as cameras, play an important role but must be monitored, provide information in real time, and cover all necessary areas of a site or venue.

AI technology is an emerging trend. Experts we interviewed noted a general increase in interest in and development of technologies incorporating some form of AI. AI-enabled video analytics can assist in identifying weapons or suspicious behavior and alert security. This could move detection farther from the site and allow for a quicker response.

Some security measures create unintended consequences. Some places, such as schools or sporting events, are meant to be open and hospitable, but some security measures, such as metal detectors, can create an atmosphere of hostility or insecurity. Additionally, security measures can create easily targeted areas outside secure areas, such as lines or crowds created by access control devices at sporting events or concerts.

Site Protection Training and Readiness

Training and response drills improve readiness and response. Training and drills can lead to fewer and less-severe casualties. This includes for facility employees, volunteers, patrons, and members of the public.

Training and assessment resources are available but not widely known. Federal agencies, such as CISA and USSS, and private companies provide training and site assessment services, but many site operators are not familiar with the types of services provided or whom to contact.

Attack Response

Cross-agency coordination and communication are critical to response. When multiple LE agencies respond to an attack, understanding who is in command, knowing what information is available, and deconflicting communications are crucial to achieving a rapid and effective response. Additionally, medical services must be able to provide medical care at the site and effectively evacuate casualties, requiring coordination with LE and other responders.

CHAPTER 4

Assessment of Preparedness and Response Spending

Grant Characterization

We reviewed available federal grant programs for their relevance in protecting or hardening ST-CPs from terrorism or violence. We present our findings in this section. The funding levels identified for each grant are for fiscal year (FY) 2023.

U.S. Department of Homeland Security Grant Programs

DHS, through FEMA, administers most of the federal grant funding aimed at protecting or hardening ST-CPs. The Homeland Security Grant Program (HSGP), Nonprofit Security Grant Program (NPSG), and Tribal Homeland Security Grant Program (THSGP) are the largest, although there are other programs administered through the agency as well.

The Homeland Security Grant Program

The HSGP is one of FEMA's grant programs that aims to enhance the ability of SLTT governments and nonprofits to prevent, protect against, and respond to terrorist attacks, including attacks on ST-CPs. Created in 2003, it consists of three components: the State Homeland Security Program (SHSP), the Urban Area Security Initiative (UASI), and Operation Stonegarden (OPSG).[1] The stated objective of the FY 2023 HSGP was "to fund SLTT efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States."[2] FEMA requires recipients to allocate 30 percent of their SHSP and UASI award funds across six priorities, five of which have minimum spend requirements of 3 percent each; the remaining 15 percent can be allocated by recipients themselves.

The national priority areas, including enhancing the protection of ST-CPs, are broken down into core capabilities and example project types. ST-CP core capabilities include opera-

[1] Operation Stonegarden "provides funding to enhance cooperation and coordination among state, local, tribal, territorial, and federal law enforcement agencies to jointly enhance security along the United States land and water borders" (FEMA, "Homeland Security Grant Program").

[2] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

tional coordination; public information and warning; intelligence and information-sharing; interdiction and disruption; screening, search, and detection; access control and identity verification; physical protective measures; and risk management for protection programs and activities. Example projects included operational overtime, physical security enhancements, security cameras, lighting, and access controls.

The State Homeland Security Program

- Agency: FEMA
- Applicability: SLTTs
- Description: "SHSP assists state, local, tribal, and territorial (SLTT) efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism."[3]
- Funding total: $415 million
- Anticipated number of grants: 56
- ST-CP mention: Yes
- ST-CP funding requirement: 3 percent of SHSP and UASI funds must be spent on "enhancing the protection of" ST-CPs.[4]

SHSP aims to enhance national preparedness for terrorism and other catastrophes. Each state or territory receives a minimum allocation of funds each year, and the balance of any funding is based on risk methodology developed by DHS. That is, each jurisdiction (the 50 states, the District of Columbia, and Puerto Rico) receives a base amount of 0.35 percent of the total funding available; American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands each receive 0.08 percent of the total funding.[5]

The Urban Area Security Initiative

- Agency: FEMA
- Applicability: States, for use in specific urban areas
- Description: "UASI assists high-threat, high-density Urban Area efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism."[6]
- Funding total: $615 million
- Anticipated number of grants: 40

[3] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

[4] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

[5] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

[6] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

- ST-CP mention: Yes
- ST-CP funding requirement: 3 percent of SHSP and UASI funds must be spent on "enhancing the protection of" ST-CPs.[7]

UASI, like SHSP, supports planning, management, and training to address threats in high-threat, high-density urban areas. Equipment purchased using UASI funding must be listed on the DHS Authorized Equipment List, including security systems, radio-frequency ID technology, and facial recognition systems. UASI funding is provided directly to the relevant state-level agency, and subrecipients (urban areas) may use funds only for purposes defined by DHS and in UASI-eligible areas. In 2023, FEMA deemed 40 areas eligible for UASI funds based on risk analysis. Allocation is based on DHS's risk methodology and expected effectiveness.[8]

Operation Stonegarden

- Agency: FEMA
- Applicability: SLTTs
- Description:

> OPSG supports enhanced cooperation and coordination among Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal, state, local, tribal, and territorial law enforcement agencies to improve overall border security. OPSG provides funding to support joint efforts to secure the United States' borders along routes of ingress/egress to and from international borders, to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders. SLTT law enforcement agencies utilize their inherent law enforcement authorities to support the border security mission and do not receive any additional authority by participating in OPSG.[9]

- Funding total: $90 million
- Anticipated number of grants: Not applicable (N/A); allocated based on risk analyses
- ST-CP mention: N/A
- ST-CP funding requirement: N/A.

The Nonprofit Security Grant Program

NSGP is another of FEMA's major grant programs that supports enhancing the ability of SLTTs and nonprofits to protect against, prepare for, and respond to terrorist and other

[7] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

[8] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

[9] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program."

extremist attacks.[10] It is broken into two funding sources for nonprofit organizations: NSGP-State (NSGP-S) and NSGP–Urban Area (NSGP-UA). The relevant state-level agency is the only entity that can apply for NSGP funding in either category on behalf of a nonprofit organization. NSGP-UA funding has to be provided to recipients in a UASI-eligible urban area. The stated objectives of NSGP are

> to provide funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist or other extremist attack. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts.[11]

The program's highest priority is enhancing the protection of ST-CPs with core capabilities, including the enhancement of planning, intelligence and information-sharing, and screening and detection.[12]

The Nonprofit Security Grant Program—State

- Agency: FEMA
- Applicability: Nonprofits outside UASI-designated high-risk urban areas
- Description: "NSGP-S funds nonprofit organizations located *outside* of a FY 2023 UASI-designated high-risk urban area. Under NSGP-S, each state will receive a target allocation for nonprofit organizations in the state located *outside* of FY 2023 UASI-designated high-risk urban areas."[13]
- Funding total: $152.5 million
- Anticipated number of grants: 56
- ST-CP mention: Yes
- ST-CP funding requirement: None.

The Nonprofit Security Grant Program—Urban Area

- Agency: FEMA
- Applicability: Nonprofits in UASI-designated high-risk urban areas
- Description: "NSGP-UA funds nonprofit organizations located *within* FY 2023 Urban Area Security Initiative (UASI)–designated high-risk urban areas."[14]

[10] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program."

[11] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program."

[12] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program."

[13] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program."

[14] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program."

- Funding total: $152.5 million
- Anticipated number of grants: 52
- ST-CP mention: Yes
- ST-CP funding requirement: None.

The Tribal Homeland Security Grant Program

- Agency: FEMA
- Applicability: Directly eligible tribes according to Section 2001 of the Homeland Security Act of 2002, as amended (6 U.S.C. § 601)
- Description: The THSGP supports FEMA's efforts to enhance the abilities of SLTTs and nonprofits to prevent, prepare for, protect against, respond to, and recover from terrorist attacks. The stated objective of the THSGP is to provide funding to directly eligible tribes ("federally recognized tribes that meet the criteria set forth in Section 2001 of the Homeland Security Act of 2002, as amended [6 U.S.C. § 601]") to strengthen their capacities to prevent, prepare for, protect against, and respond to potential terrorist attacks.[15]
- Funding total: $15 million
- Anticipated number of grants: Not mentioned
- ST-CP mention: Yes
- ST-CP funding requirement: None.

Additional Departmental Grant Programs

There are other programs that do not explicitly mention ST-CPs in their descriptions or have particular stipulations but can reasonably be considered to involve enhancing the protection of such spaces. We describe those in this section.

The Port Security Grant Program

- Agency: FEMA
- Applicability: All entities subject to an area maritime security plan, as defined by 46 U.S.C. § 70103(b), including port authorities, facility operators, and government agencies, although ferry systems that participate in the Port Security Grant Program (PSGP) will not be considered for funding under the Transit Security Grant Program (TSGP), described in the next section.
- Description: The FY 2023 program is focused on supporting increased maritime cybersecurity, managing port-wide maritime security risk, enhancing maritime domain awareness, supporting maritime security training and exercises, and maintaining or reestablishing maritime security mitigation protocols that support port recovery and resilience capabilities. In FEMA's assessment of the national risk profile for FY 2023,

[15] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Tribal Homeland Security Grant Program."

two areas warrant the most concern: (1) enhancing cybersecurity and (2) enhancing the protection of ST-CPs.
- Funding total: $100 million
- Anticipated number of grants: N/A
- ST-CP mention: Yes
- ST-CP funding requirement: N/A, but each applicant receives a 20-percent increase to its scores for addressing one or both of the national priorities (enhancing cybersecurity and enhancing protection of ST-CPs) in its investment justifications. Any project submitted by a public-sector applicant or otherwise certified by the U.S. Coast Guard Captain of the Port as having a port-wide benefit will have its final scores increased by 10 percent.

The PSGP is one of four FEMA grant programs focusing on transportation infrastructure security. Authorized by Congress, "[t]he PSGP provides funds to state, local, territorial, and private sector partners to support increased port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism."[16] The PSGP focuses on enhancing maritime domain awareness, port resilience, training, and transportation ID credential implementation. Any entity required to have an area maritime transportation security plan, including a port authority, is eligible to apply.

The Transit Security Grant Program

- Agency: FEMA
- Applicability: Limited to named passenger rail, intracity bus, and ferry systems in particular urban areas
- Description: The TSGP is one of four grant programs implementing FEMA's focus on transportation infrastructure security activities. This grant provides "funds to eligible public transportation systems (which include intra-city bus, ferries, and all forms of passenger rail)" to increase the resilience of transportation infrastructure and "protect critical transportation infrastructure and the traveling public."[17]
- Funding total: $93 million
- Anticipated number of grants: N/A
- ST-CP mention: Yes
- ST-CP funding requirement: N/A, but an applicant receives a 20-percent increase to its scores for addressing one or both of the national priorities (enhancing cybersecurity or enhancing protection of ST-CPs) in its investment justifications.

The TSGP provides owners and operations of transit systems (e.g., commuter buses, ferries, rail, intracity bus) funding to "protect critical surface transportation infrastructure and

[16] FEMA, "FY 2023 Port Security Grant Program Fact Sheet."

[17] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Transit Security Grant Program."

the traveling public from acts of terrorism." Eligibility is determined by "ridership and transit systems that serve historically eligible Urban Area Security Initiative (UASI) urban areas."[18] DHS uses a competitive, risk-based process to award funds.

The Intercity Passenger Rail Program

- Agency: FEMA
- Applicability: Only the National Railroad Passenger Corporation (Amtrak)
- Description:

> The Inter-City [sic] Passenger Rail (IPR) Program directly supports transportation infrastructure security activities for the Amtrak System and is one tool in the comprehensive set of measures authorized by Congress and implemented by the Administration to strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks.[19]

- Funding total: $10 million made available in FY 2021 via congressional direction
- Anticipated number of grants: 1
- ST-CP mention: Yes
- ST-CP funding requirement: 5 percent.

Congress created an IPR Program to increase sustainable, risk-based efforts to curtail vulnerabilities in critical surface transportation. Amtrak is the only entity allowed to apply for the $10 million funding.

The Intercity Bus Security Grant Program

- Agency: FEMA
- Applicability: Any private, intercity bus operator that has also completed a vulnerability assessment and developed a security plan that has been approved by the Secretary of Homeland Security and operates in one of more historically eligible UASI urban areas or operates a charter bus service that provides at least 50 trips annually to one or more historically eligible UASI urban areas
- Description: This grant "provides funds to eligible intercity bus companies to protect critical transportation infrastructure and the travelling public from acts of terrorism."[20]
- Funding total: $2 million
- Anticipated number of grants: N/A
- ST-CP mention: Yes

[18] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Transit Security Grant Program."

[19] Grants Office, "Intercity Passenger Rail (IPR) Program."

[20] Grant Programs Directorate, "The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Intercity Bus Security Grant Program."

- ST-CP funding requirement: N/A, but an applicant receives a 20-percent increase to its scores for addressing one or both of the national priorities (enhancing cybersecurity or enhancing protection of ST-CPs) in its investment justifications.

Finally, the Intercity Bus Security Grant Program provides funding to enhance the protection of intercity bus systems and the public. Eligible applicants include operators of intercity and charter buses operating in UASI-eligible urban areas.

U.S. Department of Transportation Programs

The U.S. Department of Transportation, through the Federal Transit Administration, administers the Capital Investment Grants program, which provides funding for heavy rail, commuter rail, light rail, street cars, and bus rapid transit. Transit systems throughout the country and selected territories are eligible to apply.[21]

Similarly, the Federal Aviation Administration, through the Airport Improvement Program, provides grants to assist public-use airports with enhancing airport safety, capacity, security, and environmental concerns. Eligible applications are limited to public-use airports included in the National Plan of Integrated Airport Systems.[22]

U.S. Department of Justice Programs

The U.S. Department of Justice's Students, Teachers, and Officers Preventing (STOP) School Violence Act Program is also relevant. Programs funded with grants from this program include the School Violence Prevention Program, administered by the Office of Community Oriented Policing Services, which aims to improve security at schools with a focus on physical security measures, training, and emergency communications. Eligible applicants include local school districts, police departments, and state and local governments.[23]

Findings About Grants

These federal grant programs offer billions in funding to SLTT governments, nonprofit organizations, and other entities to operate critical infrastructure, mass-transit systems, and schools. These funds are meant to be used to harden ST-CPs and the public from terrorism, mass violence, and other threats. Much information is available about these funds and programs, including qualifying applicants, administration of funds, and criteria for successful applications. What is not available, however, is any account of how funds are spent once they are allocated to applicants. Indeed, a SME we interviewed indicated they were not aware of any mechanism for the review of spending of public grant monies. We attempted to but were

[21] Federal Transit Administration, "Capital Investment Grants Program."

[22] Federal Aviation Administration, "Airport Improvement Program (AIP)."

[23] Office of Community Oriented Policing Services, "School Violence Prevention Program (SVPP)."

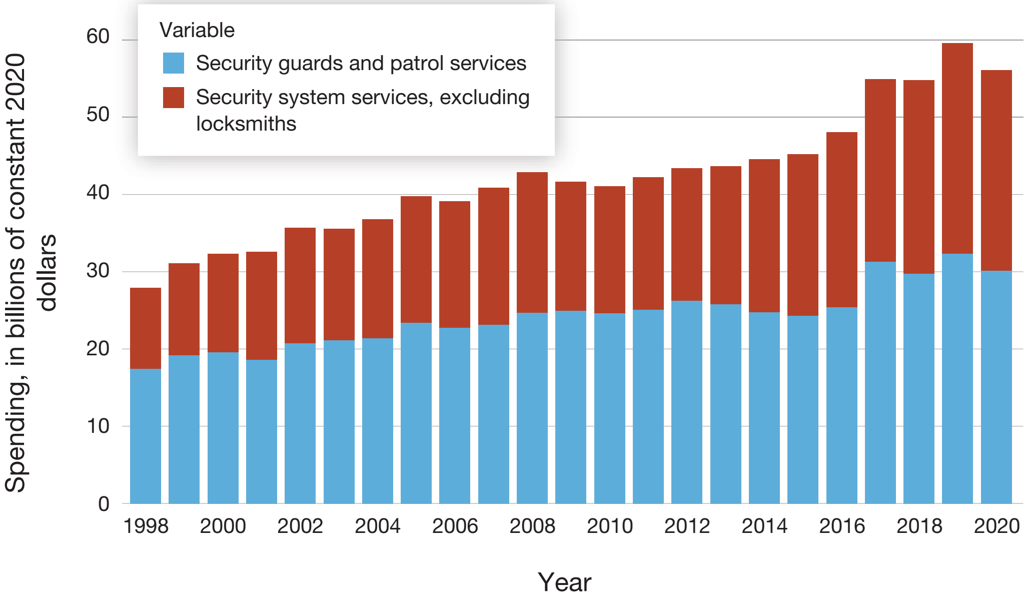
unable to discover any publicly available information on the allocation of grant funds by government and other organizations. In short, given the dearth of information after grant funds are awarded, drawing more-meaningful conclusions about how grant funds are actually spent and assessing their utility are difficult. To that end, we make the following recommendations:

- Require grant awardees to report their spending to DHS using a framework or mechanism that ensures that funds meant for enhancing the protection of ST-CPs are spent as intended.
- To the extent practical, make grant-spending information available for review by Congress, the public, and other interested parties. This could have the added benefit of ensuring that trends or gaps in spending on the protection of ST-CPs can be noted, and such information could play a role in enhancing the cooperation of SLTTs.

An Analysis of Historical Security Spending

In this section, we present the aggregate historical private security spending results from our top-down analysis described previously. Aggregate security spending is illustrated in Figure 4.1 and shows significant growth since the U.S. Bureau of Labor Statistics began tracking such spending in 1998. Between 1998 and 2020, revenue in these two sectors increased

FIGURE 4.1
Aggregate Security Spending



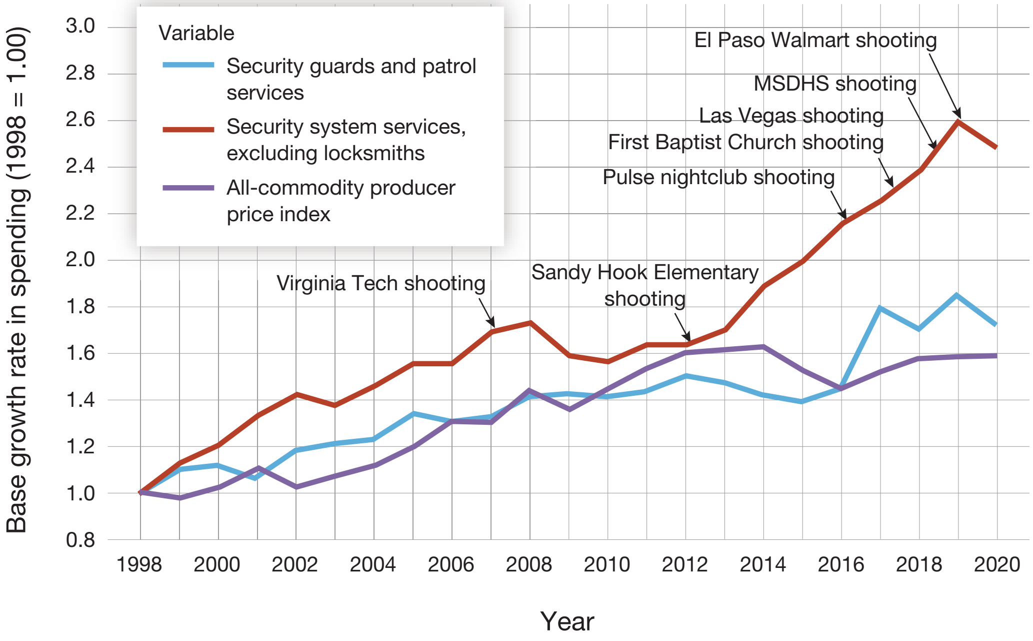
SOURCE: Features information from U.S. Census Bureau, "Investigation and Security Services, All Establishments, Employer Firms."

from approximately $28.0 billion to $59.6 billion (in 2020 dollars). Also, these data show that the category of security guards and patrol services has historically made up a larger share of security spending than other categories—approximately 58 percent of the aggregate security spending, on average, each year.

In Figure 4.2, we present the normalized revenue to better understand trends in security spending. These data show that, although the category of security guards and patrol services has historically made up a larger share of security spending than other categories, this trend is reversing, and the security-system category is accounting for an increasing share of overall security spending, which is rapidly outpacing the spending in the categories of all commodities and of security guards and patrol services by about 56 percent.

There is an inflection point after the Sandy Hook school shooting in 2012. Spending on security systems rose approximately 52 percent, with spending on guards and patrols increasing approximately 15 percent, until 2020. In 2020, total spending reached $56.2 billion, with $30.2 billion in guard and patrol services and $26.0 billion in security services.

FIGURE 4.2
Trends in Security Spending



SOURCE: Features information from U.S. Census Bureau, “Investigation and Security Services, All Establishments, Employer Firms.”

NOTE: The First Baptist shooting was in Sutherland Springs, Texas, on November 5, 2017.

Preliminary Security Cost Models

In this section, we present the results from a bottom-up approach to estimating costs for school safety and security hardening measures. Table 4.1 gives an overview of the total annualized costs in 2022 dollars on a per-school level, per–school district level, and a national level across the portfolio of K–12 public schools in the United States, which are estimated at $251,600, $3.2 million, and $20.5 billion, respectively. These ranges for cost estimates assume a mean unit cost and mean unit of quantity. The corresponding nonlabor portions of these costs are provided in Table 4.2.

The cost model accounts for uncertainty in both the unit cost (i.e., the cost per item identified) and the unit quantity (i.e., the number of each item identified assumed for the cost estimate). Calculating cost estimates for the 21 possible combinations of unit cost and unit quantity resulted in a range of total costs for each cost category. For instance, in one scenario, we could assume a minimum unit cost and a maximum unit quantity to estimate the total costs for safety and security hardening measures; in another scenario, we could assume a mean unit cost and a minimum unit quantity to estimate the total costs. Figure 4.3 illustrates

TABLE 4.1

Total Cost for School Safety and Security Hardening Measures, in Millions of Dollars

	Total Annualized Cost		
Cost Level	Mean	Minimum	Maximum
Individual school	0.2516	0.1133	0.5070
School district	3.2	2.4	5.3
All schools in the United States	20,200	8,000	39,700

NOTE: Values presented for mean, minimum, and maximum are based on the respective unit cost and unit quantity for each group (i.e., values in the “Mean” column represent a mean unit cost and a mean unit quantity).

TABLE 4.2

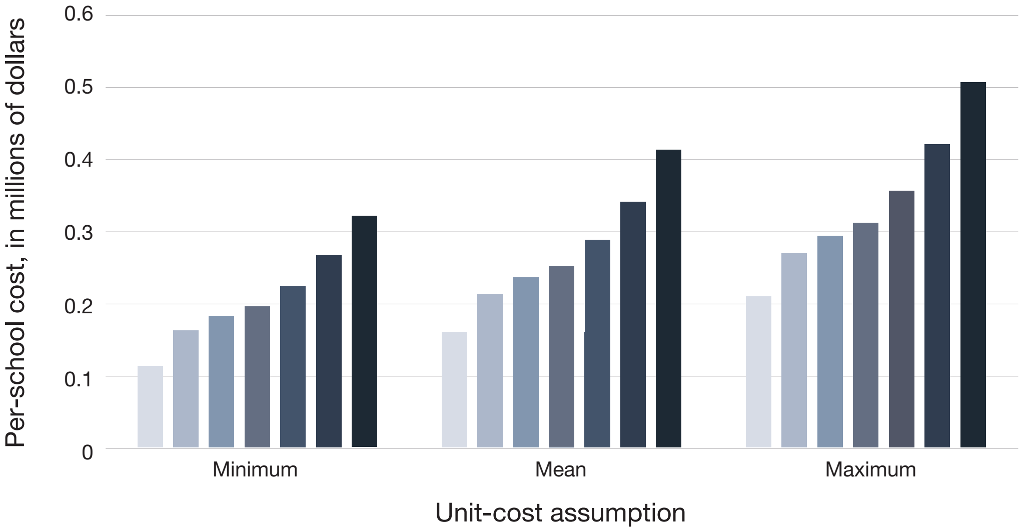
Total Cost for Nonlabor Elements of School Safety and Security Hardening Measures, in Millions of Dollars

	Total Annualized Cost		
Cost Level	Mean	Minimum	Maximum
Individual school	0.0443	0.0155	0.1055
School district	0.4871	0.1708	1.2
All schools in the United States	4,200	1,500	10,100

NOTE: Values presented for mean, minimum, and maximum are based on the respective unit cost and unit quantity for each group (i.e., values in the “Mean” column represent a mean unit cost and a mean unit quantity).

FIGURE 4.3

Range of Annualized Costs per School for Safety and Security Hardening Measures, in Millions of Dollars



NOTE: Each unit-cost group (minimum, mean, and maximum) includes a range of annualized costs based on a range of assumptions for the unit quantities (minimum to maximum).

the range of total annualized costs to implement school safety and security hardening measures on a per-school level for the 21 possible combinations of unit cost and unit quantity.

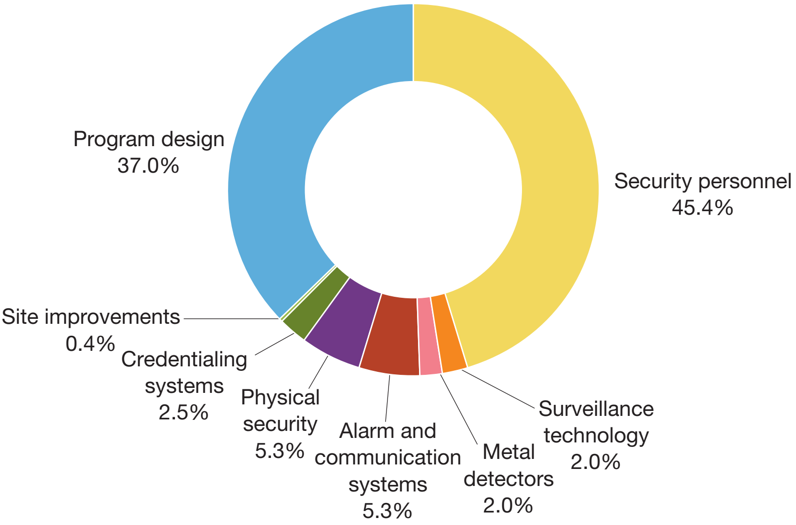
The ranges of annualized costs per school illustrated in Figure 4.3 are grouped by the three assumptions of unit cost (i.e., minimum, mean, and maximum) and the varying assumptions of unit quantities (i.e., minimum to maximum). Several factors, such as the size of the school, location of the school (e.g., urban versus rural), or material specifications (e.g., high-end locksets versus industry-standard locksets), can affect the calculus of the total cost.

Figure 4.4 illustrates the breakdown of the total annualized costs for an individual school by cost category. A significant portion of the total costs for safety and security hardening measures is due to labor for security guards (approximately 45 percent) and resources for school safety and security programs, such as training school staff (approximately 37 percent). These percentages vary depending on what assumptions are made for the unit cost and unit quantity. For example, if we assume a minimum unit cost and a minimum unit quantity, the percentage of total annualized costs that are attributed to labor and program design increases to 86 percent, as compared with 82 percent when assuming a mean unit cost and a mean unit quantity. However, in all the combinations of unit cost and unit quantity, security guard labor and program design costs remain a high percentage of the total annualized costs.

Cost categories related to physical infrastructure improvements, such as security fencing, site lighting, or updated doors, represent a smaller percentage of the total annualized costs. Figure 4.5 illustrates the breakdown of total annualized costs for physical infrastruc-

FIGURE 4.4

Annualized Costs for School Safety and Security Hardening Measures, by Cost Category



NOTE: The breakdown presented in this figure is based on annualized cost per school assuming a mean unit cost, a mean unit quantity, and implementation of all safety and security hardening measures. Percentages do not sum to 100 because of rounding.

ture improvements (i.e., excluding costs for security guards and program design). The cost model does not consider the effectiveness of the security and safety measures, which would be important information to have for school safety decisionmaking. For example, although annualized costs for surveillance technology per school (approximately 2 percent) are similar to annualized costs for credentialing systems (approximately 2.5 percent), a properly designed and implemented credentialing system in a school might be a more effective deterrent from a potential mass attack than security cameras would be.

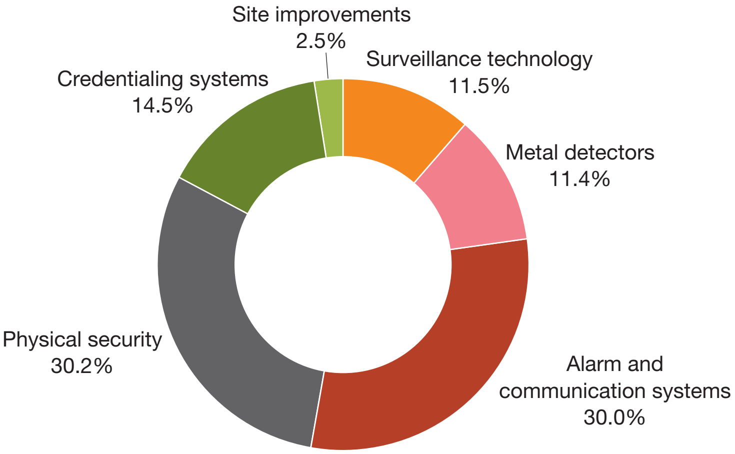
An Overview of K–12 Site Security Costs

Together, these analyses of spending on security provide estimates for the scale of spending on school security nationally, the sources of those costs, and the nature of trends in this spending. Aggregate economic data suggest that spending on security in the United States has grown to tens of billions of dollars annually, reaching as high as $56 billion in 2020. Although these numbers are an overestimate of spending in schools, they provide an upper bound for consideration and highlight trends in spending that are likely relevant for school security as well.

These costs represent predominantly spending on security guards and patrol services rather than security systems. Spending on security systems has risen rapidly since about 2012, following several high-profile mass attacks in public spaces. This rise in spending on

FIGURE 4.5

Annualized Costs for School Safety and Security Hardening Measures Related to Physical Infrastructure Improvements, by Cost Category



NOTE: The breakdown presented in this figure is based on annualized cost per school assuming a mean unit cost, a mean unit quantity, and implementation of all safety and security hardening measures. It excludes costs for security guard labor and program design. Percentages do not sum to 100 because of rounding.

security systems could be explained by either heightened awareness of security vulnerabilities, adoption of new security standards for public spaces, technological advances making new security systems available and affordable, or a combination of these factors.

Cost modeling of guard services and security systems for schools provides a broad range of potential national costs that serves as a contrast to the cost estimate provided from aggregate economic data. The full range of costs provided by this modeling ranges from around $8 billion to around $40 billion when considering uncertainty in unit costs, unit quantities, variation in schools across the country, and variation in security measure adoption across school districts. As observed with aggregate security economic data, most of these costs are associated with security guard and program design costs. Thus, an estimate for the annualized cost of security systems in schools across the United States ranges from about $1.5 billion to $10 billion. This is a potentially upper-bound, albeit believable, cost estimate, considering the insight gained into security spending from aggregate economic data. Uncertainty in this estimate could be resolved by gaining a better understanding of the status and trends in adoption of security measures across schools.

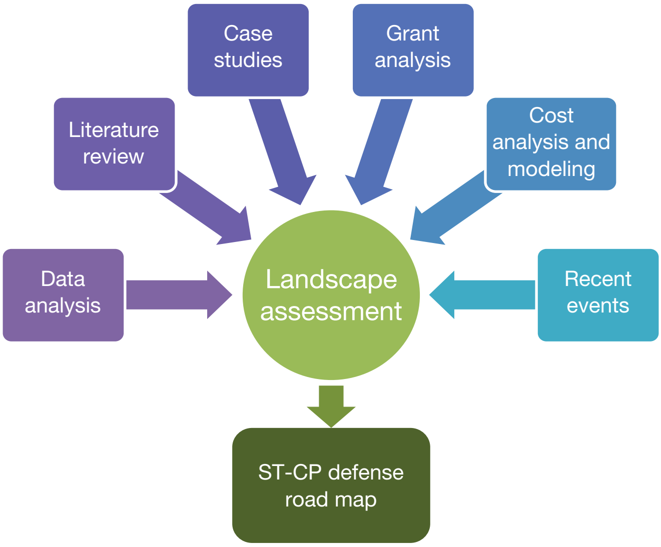
CHAPTER 5

Findings

A Landscape Assessment to Assess the Effectiveness of Security Procedures and Technologies

Using the results of the other tasks, we performed a landscape assessment of ST-CP risks and security, illustrated in Figure 5.1. This analysis is intended to create a summary, conceptual picture or model of the state of ST-CP attacks and security, covering attack risks and corresponding prevention and protection measures. It includes a synthesis of findings from the other tasks. It also incorporates lessons learned from events that are too recent to be included in the latest scholarly literature and datasets. As the conceptual model is assembled, the analysis further includes a logical analysis of how well the various elements and relation-

FIGURE 5.1
Landscape Assessment Methodology



ships in the model are working, where there are gaps, and candidate solutions to address the problems. The resulting model becomes the landscape.[1]

The next step in our assessment, developing the road map, consists of developing the candidate solutions, providing more details, and explaining known needs, for implementation. The road map also prioritizes the potential solutions, flagging those that seem to be most critical. In this report, the main driver of criticality is whether the gap is fundamental (i.e., little exists to fill the gap) or there are existing solutions that just need improvements. The road map also sequences the candidate solutions, identifying which should come first because they are more foundational and needed for later solutions, as applicable.

A Conceptual Model of Attacks on and Security Measures for Soft Targets and Crowded Places: Layers of Security Forming a System-Based Approach to Prevention and Protection

Previous HSOAC research has developed the concept of layers of security around a building or site of interest, with the idea being that an attacker would have to breach all these layers in whole or in part to attack a site successfully. Previous work modeled defensive layers spatially, showing them on stylized site plans. Figure 5.2 provides an example plan, based on ASIS International standards and guidelines and on prior HSOAC research.[2] This site plan is based on school security research, although most layers are also applicable to other types of ST-CPs.

We modified this concept to reflect attackers' actions and corresponding security responses from a process perspective. We first characterized an *ST-CP attack chain*: a set of conditions that a would-be attacker must fulfill to successfully carry out an ST-CP attack with a high number of fatalities:

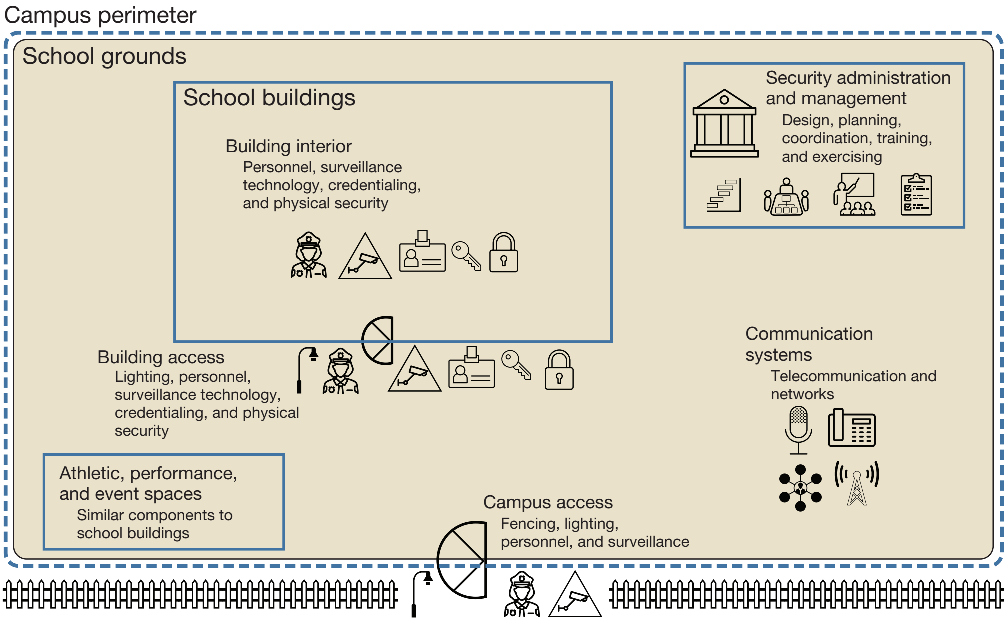
- The attacker must be motivated to the point of being fully committed to an attack.
- The attacker must carry out advance preparation: conducting the planning (likely to include gaining weapon skills and an understanding of the target site, possibly attempting to recruit others), acquiring materiel (most frequently guns, ammunition, and clips), and making other logistical preparations (travel). They must do all of this without being detected, reported, or interdicted by others.
- Once on scene, the attacker must get through whatever layers of entry and interior site security are present and must attack without being stopped by on-scene security or civilian bystanders.

[1] The specific data collection, representation, and diagramming techniques used in a landscape assessment vary based on the subject of the analysis. Identifying the core narrative and corresponding diagrams that reasonably explain the phenomena being analyzed is a core part of landscape assessment.

[2] ASIS International, *Physical Asset Protection*; ASIS International, *Protection of Assets*; Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

FIGURE 5.2

A Spatial Representation of Security Layers in Soft Targets and Crowded Places: A School Model


Campus perimeter
School grounds
School buildings
Building interior
Personnel, surveillance technology, credentialing, and physical security
Security administration and management
Design, planning, coordination, training, and exercising
Building access
Lighting, personnel, surveillance technology, credentialing, and physical security
Communication systems
Telecommunication and networks
Athletic, performance, and event spaces
Similar components to school buildings
Campus access
Fencing, lighting, personnel, and surveillance

SOURCE: Features information in Moore et al., *A Systems Approach to Physical Security in K–12 Schools*.

- Finally, to maximize casualties, the attacker needs to find a crowd and extend the attack time to attack as many as possible and convert as many injuries into deaths as possible (such as by preventing LE and medical response for as long as possible).

Importantly, an attacker can be stopped (or at least casualties can be reduced) at any of these points. The specific measures that can detect and stop attackers can be grouped, by attack step, into layers of defense (or security). Assuming that these measures are coordinated, the measures at each layer collectively form a system for ST-CP security.

From our analyses, we make this overall finding: **System-based approaches to prevention and protection are likely to yield the most benefits**, described as follows:

- Under a system approach, physical security technology, site and building design features, personnel, policies and procedures, and training programs work cohesively to provide maximum security benefits.
- A layered approach to security helps avoid having single points of failure while increasing the likelihood of attack failure; it ensures that elements are working in an integrated way to deter, detect, delay, and respond to threats.

- A system-based approach can be tailored to help diverse STs address their unique circumstances and ensures that security measures work with parallel efforts (e.g., violence prevention, response, and recovery).
- To manage the system, a multidisciplinary team leading the planning process for the system-based approach helps meet the requirements of diverse stakeholders and enhances response capabilities.

As described in the literature review section in Chapter 1, there is a substantial body of work describing the value, benefits, and importance of layered or system approaches to site security.

Figure 5.3 shows the steps in the ST-CP attack chain, along with the layers of security for each step. There are four categories of defensive layers:

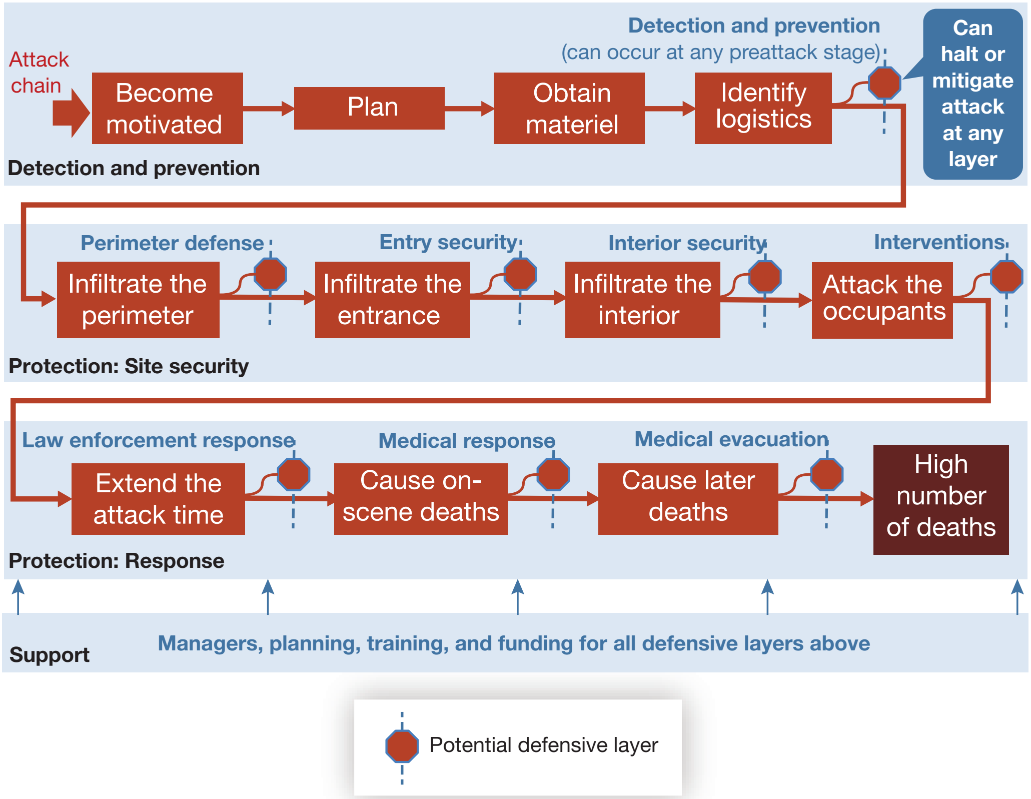
- **Prevention layers** are intended to prevent attacks from occurring in the first place, either by finding and interdicting would-be attackers in advance or by dissuading or deterring them from committing to an attack at all.
- **Protection through site security layers** is intended to thwart the initial stages of a mass attack on an ST-CP, using various on-site security measures.
- **Protection through response layers** is intended to stop a mass attack underway as quickly as possible and minimize fatalities and other casualties in the process.
- Finally, the **support category** provides the management, coordination, planning, training, and funding necessary to field and maintain the other layers.

The following sections describe the attack chain steps and defensive layers in more detail; they also indicate what is needed to improve them.

The Prevention Layers of Security

The top half of Figure 5.4 shows the steps carried out in preparation for an ST-CP attack. It also shows observable indicators of each of these steps, which are what will be reported as tips from the public or discoveries by LE. Core to these observable indicators is the concept of *leakage*—when a would-be attacker lets others know of their intentions and plans either in person or (increasingly) online via social media. The bottom half shows the *prevention* portion of the defense chain—those steps that authorities need to take to detect and act on the observable indicators to thwart a would-be plot.

FIGURE 5.3
The Attack Chain and Corresponding Defensive Layers for Soft Targets and Crowded Places



Issues Involving Prevention Measures

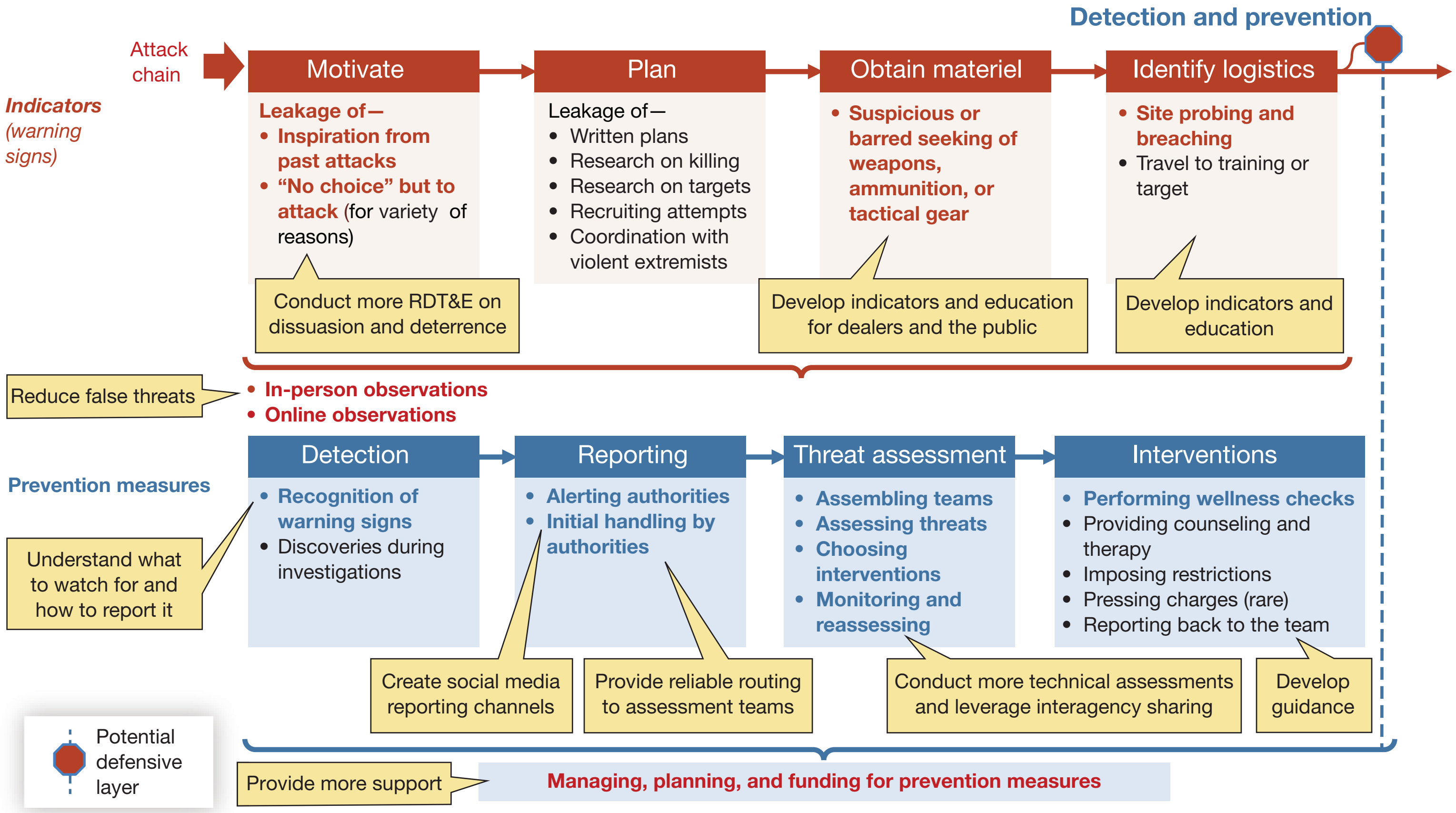
Detection and Reporting: A Need for More Knowledge About What to See and How to Say It

As discussed earlier, tips from the public are the main source of the initial clues leading to foiling attack plots. There is thus a strong need to build on the ubiquitous "see something, say something" axiom with more information on what to see—top indicators of potential plots—and how to say it—how to report it to authorities:

- For observation, we noted a need to educate specifically on the types of clues for attacks by adults outside of schools (who are not being regularly monitored by authorities and peers), such as online threats or leakage, suspicious acquisition of weapons, or site probing.
- For reporting, we identified a specific need to publicize reporting channels; in some cases, a reporter was unsure of the criticality and thus did not want to report it to 911.

FIGURE 5.4

Prevention Layers of Security and Issues



Detection and prevention
Attack chain
Motivate
Plan
Obtain materiel
Identify logistics
Indicators (warning signs)
Leakage of—
• Inspiration from past attacks
• "No choice" but to attack (for variety of reasons)
Leakage of—
• Written plans
• Research on killing
• Research on targets
• Recruiting attempts
• Coordination with violent extremists
• Suspicious or barred seeking of weapons, ammunition, or tactical gear
• Site probing and breaching
• Travel to training or target
Conduct more RDT&E on dissuasion and deterrence
Develop indicators and education for dealers and the public
Develop indicators and education
Reduce false threats
• In-person observations
• Online observations
Prevention measures
Detection
Reporting
Threat assessment
Interventions
• Recognition of warning signs
• Discoveries during investigations
• Alerting authorities
• Initial handling by authorities
• Assembling teams
• Assessing threats
• Choosing interventions
• Monitoring and reassessing
• Performing wellness checks
• Providing counseling and therapy
• Imposing restrictions
• Pressing charges (rare)
• Reporting back to the team
Understand what to watch for and how to report it
Create social media reporting channels
Provide reliable routing to assessment teams
Conduct more technical assessments and leverage interagency sharing
Develop guidance
Potential defensive layer
Provide more support
Managing, planning, and funding for prevention measures

NOTE: Bold signals that we identified an issue (typically a gap) with that indicator or prevention step; the callouts indicate ways to close the gaps.

There were also needs to publicize conditions and assurances under which the person being reported was very unlikely to be arrested.

Detection: A Need to Reduce False Threats

Discussion at the 2023 NIJ conference included multiple comments that authorities in schools and elsewhere were being overwhelmed with false threats to carry out mass shootings (sample paraphrase: *Kids used to call in false bomb threats to get out of math tests or lash out at peers or teachers they didn't like—now they call in false mass-shooting threats, which are much more serious*). Having to assess and intervene with students or others making false threats was described as taking up valuable resources that could be much better spent on the few true threats.

Reporting: A Need to Improve Channels for Social Media Reporting

Tips from the public are increasingly based on leakage of attack plans or preparations online. However, we identified as a gap a lack of easy ways to report such leakage to authorities; it is commonly possible to flag attack threats for violating terms of service, for example, but not to report such threats to authorities for validation.

Assessment: A Need for More Technical Assessments and Interagency Sharing

We identified needs to provide more-rigorous frameworks and documentation tools to help assessment teams determine how much of a threat a reported person poses and what next steps should be taken. We similarly identified needs to improve interagency coordination and sharing to improve the completeness of information used to make those assessments (i.e., better "connect the dots").

Interventions: Guidance on Wellness Checks

Conducting initial welfare checks on reported people to provide initial in-person characterizations of how much of a threat someone might pose and determine any needed interventions is an inherent part of prevention. However, we were not able to locate guidance on how to conduct these checks.

Funding and Support for Assessment Teams

Finally, we identified needs to improve funding and support for the multidisciplinary teams responsible for handling the incoming tips and carrying out the assessments and actions that lead to attacks being foiled.

Issues Involving Attackers' Actions and Observability

Attackers' Motivation: A Need for More Understanding of Dissuasion and Deterrence

We studied predominantly detection of an attack plot once an attacker has decided to commit to it. We identified a need for research to identify interventions that could help dissuade or deter someone from carrying out an attack to begin with. Researchers with the nonprofit Violence Project conducted an NIJ-funded study of the life histories of 194 mass shooters and identified the following core life cycle:

- *childhood trauma*, with "adverse childhood experiences" being common
- *personal crisis*, with attackers reaching a "breaking point," often including suicidality (31 percent expressing suicidal intentions before the attack and 40 percent during the attack[3])
- *social proof*, in which a would-be attacker gets inspiration and validation for carrying out a mass attack, often online, with the validation being ideological (radicalization) or more broadly idealizing of past mass shooters and mass violence[4]
- *opportunity*, in which attackers gain the weapons and make other logistical preparations needed to carry out attacks.[5]

Early trauma and personal crises, as well as some degrees of suicidal ideation, are extremely common—however, most of the tens of millions of Americans suffering from these do not go on to become mass attackers. The social proof and opportunity phases appear to be much rarer and hence more actionable. Although detecting indicators of attack preparation (opportunity) are covered by the Violence Project study and others, more work should be done on how to break the social proof stage and increase deterrence and dissuasion of attacks. This is especially important given signs that social proof encouraging attackers has been increasing in recent years and thus could be behind increases in the numbers of mass-attack plots and casualties.[6]

Indicators of and Education About Suspicious Seeking of Weapons and Ammunition

Core to carrying out mass shootings on ST-CPs is acquiring the weapons and ammunition to do so. We found that, for those plots in which the sources of the weapons could be tracked, federally licensed dealers and thefts from family and associates were major sources of such weapons. We also found little existing material on the warning signs of someone attempt-

[3] Violence Project, "Key Findings."

[4] There is some evidence that saturation of media coverage and societal reaction to mass attacks can also incentivize attackers, who see the reaction as showing a way to become famous. See, for example, Lankford and Silver, "Why Have Public Mass Shootings Become More Deadly?" One potential solution to this, suggested in Lankford and Madfis, "Media Coverage of Mass Killers," is a no-notoriety approach to covering mass attackers.

[5] Peterson, "The Violence Project."

[6] Lankford and Silver, "Why Have Public Mass Shootings Become More Deadly?" Also, Violence Project, "Key Findings," notes an increase in attacks motivated by hate and fame-seeking since 2015.

ing to acquire weapons and ammunition for attacks or on how to report them.[7] Identifying attempts to acquire large stockpiles of ammunition and clips appears to be a special opportunity because there can be cases in which an active shooter has ready access to the guns (e.g., family-owned weapons) but not to the massive amounts of ammunition and clips they carried during attacks. There is a strong need for both RDT&E to identify key indicators of gun and ammunition diversion without unduly hampering legitimate purchases (for, e.g., hunting, sporting) and development of subsequent education campaigns.[8]

Indicators and Education on Site Probing and Breaching

Carrying out advance reconnaissance of attack sites is an inherent part of mass-attack preparation. However, the MADT dataset includes few examples of plots being found via on-scene surveillance and probing, implying that there is an opportunity to find more plots by improving detection of these activities.

Protection: On-Site Security Layers

As shown in Table 5.1, security measures in each defensive layer are divided into three categories, depending on the extent of measures typically present in each.

Figure 5.5 shows the initial steps an attacker carries out to get through on-site security and start attacking a crowd, along with corresponding defensive layers.

Security measures in these categories typically are cumulative; a site in each category typically uses both the measures listed in its row plus the measures in the prior categories above.

Issues Involving the Security of Open Spaces

A Need to Develop Security Concepts for Open and Nonsecured Spaces

Most research and articles we identified were about secured buildings or major venues; we found little specifically on how to secure open spaces and nonsecured buildings that, almost by definition, do not have more-intensive security measures. What little is present sometimes includes surveillance cameras and other sensors (for areas that have shot detection). The only reliable security measure present, however, is the bystanders themselves. Thus, measures

[7] Exceptions include training by the National Shooting Sports Foundation, “5 Ways the Firearm Industry Is Helping to Keep Guns Out of the Wrong Hands,” and the National Crime Prevention Council, “Sell with Certainty.” However, the National Shooting Sports Foundation’s campaign focuses on detecting straw purchasers (that is, someone purchasing a gun for someone who could not legally do so themselves), and the Sell with Certainty campaign focuses on getting private individuals to sell their weapons back to federally licensed dealers.

[8] Although identifying excessive ammunition purchases could be a method of flagging suspicious behavior, many of the types of attacks examined in this report could be carried out with relatively small amounts of ammunition. Purchasing several 100-round boxes of ammunition at a local gun store or online would not raise suspicion but would still provide enough ammunition to carry out an attack.

TABLE 5.1
Security Measures in Each Defensive Layer for Each Type of Soft Target or Crowded Place

ST-CP Type	Description	Security Measure
Open space	Includes streets, parking lots, and parks but also includes typically unsecured, public-access buildings (e.g., shopping malls, bars, restaurants). These spaces are easier to flee and thus harder to secure than secured buildings or major venues. They can lack defined perimeters, entries, and interiors.	Typically includes surveillance cameras, perimeter barriers (e.g., fencing), and guards or off-duty officers who happen to be on-scene. The consistent defensive measure present is bystanders.
Secured building	Includes schools and workplaces	Is intended to keep out those who are not part of the organization housed in the building. At a minimum, these have controlled access measures; they frequently have guards, stockpiled medical supplies, and people with some emergency first aid training as well.
Major venue	Includes arenas, theme parks, and airports	Is intended to screen people arriving on site for weapons and other contraband, in addition to controlled access and guards. They might have police and medical personnel stationed during major events as well. These presences can provide a deterrent effect.

are most needed that provide the public with education and tools to report attackers more quickly or respond more effectively (either by leaving the scene earlier or physically halting the attacker).

For these concepts, planners must consider options and conditions for upgrading the security of open sites in a cost-effective, nonintrusive matter. The literature review and detailed case studies, for example, pointed out possibilities for adding perimeter protections, additional entryways, layers of doors (external and internal), alarms, and capabilities to lock doors quickly.

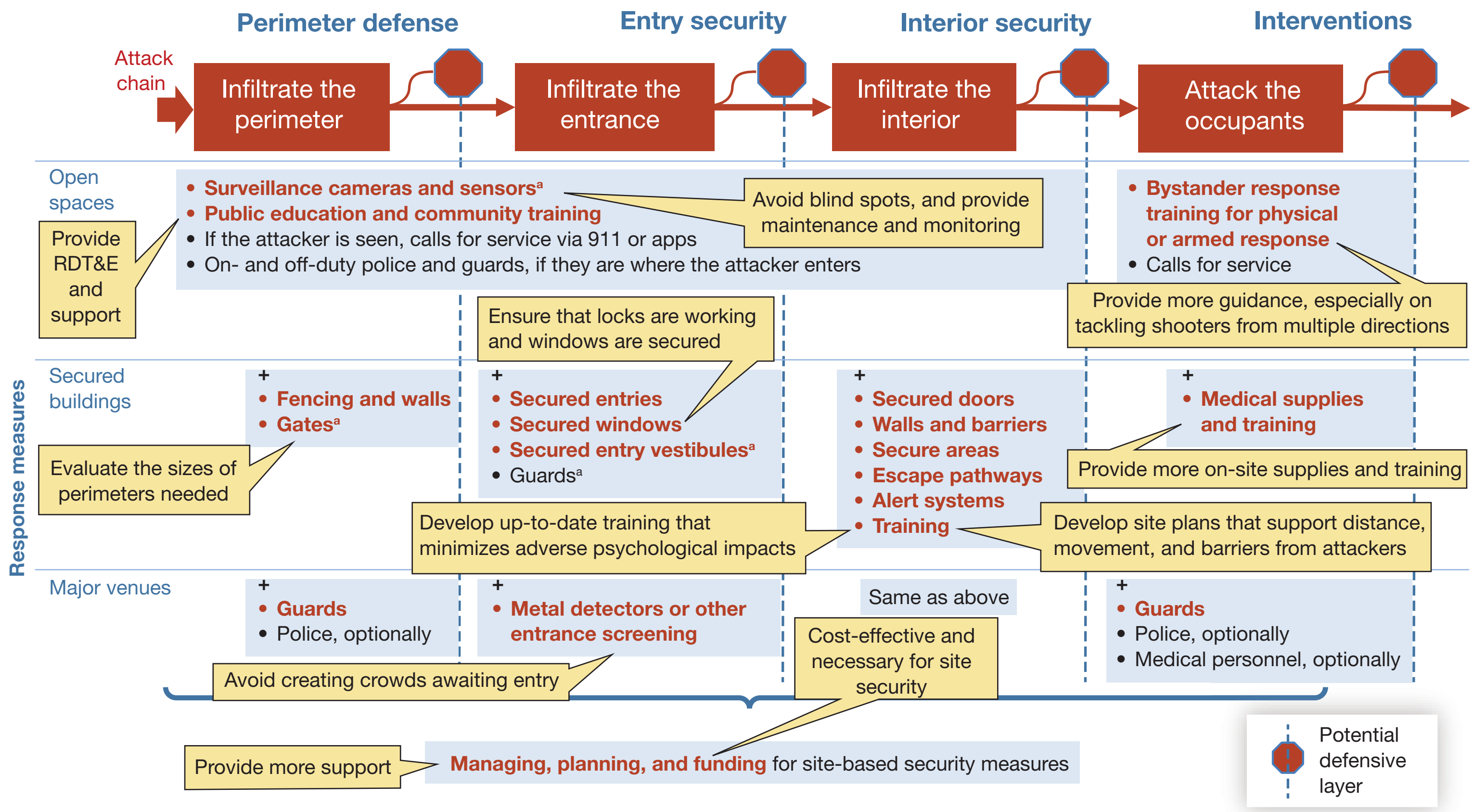
A Need to Improve Bystander Response

Our analysis largely validated the DHS concept of "run, hide, and fight," with the exception that there needs to be clarification that "run" can mean running to a secure location and "hide" means getting to a secure location where the shooter is very unlikely to find the person (i.e., not hiding under a table or desk in open view of a shooter). From examining how bystanders responded to shooters and outcomes, however, we found that the public needs more detail on "fight." Instructions need to be provided or improved on the following:

- It needs to be made clear that, **if someone is in close range of a shooter, they are in a "fight" situation and must respond with overwhelming physical force**. Effectively, people must respond to a mass shooter the same way they would respond to someone trying to hijack an airliner post-9/11.

FIGURE 5.5

Protection: Site-Based Layers of Security and Issues


Perimeter defense
Entry security
Interior security
Interventions
Attack chain
Infiltrate the perimeter
Infiltrate the entrance
Infiltrate the interior
Attack the occupants
Response measures
Open spaces
• Surveillance cameras and sensors[a]
• Public education and community training
• If the attacker is seen, calls for service via 911 or apps
• On- and off-duty police and guards, if they are where the attacker enters
• Bystander response training for physical or armed response
• Calls for service
Provide RDT&E and support
Avoid blind spots, and provide maintenance and monitoring
Provide more guidance, especially on tackling shooters from multiple directions
Ensure that locks are working and windows are secured
Secured buildings
+
• Fencing and walls
• Gates[a]
+
• Secured entries
• Secured windows
• Secured entry vestibules[a]
• Guards[a]
+
• Secured doors
• Walls and barriers
• Secure areas
• Escape pathways
• Alert systems
• Training
+
• Medical supplies and training
Evaluate the sizes of perimeters needed
Provide more on-site supplies and training
Develop up-to-date training that minimizes adverse psychological impacts
Develop site plans that support distance, movement, and barriers from attackers
Major venues
+
• Guards
• Police, optionally
+
• Metal detectors or other entrance screening
Same as above
+
• Guards
• Police, optionally
• Medical personnel, optionally
Cost-effective and necessary for site security
Avoid creating crowds awaiting entry
Provide more support
Managing, planning, and funding for site-based security measures
Potential defensive layer

NOTE: Bold type signals that we identified an issue (typically a gap) with that indicator or prevention step; the callouts indicate ways to close the gaps. + = Add these items to the ones above (e.g., the perimeter-defense response measures for secured buildings consist of those for open spaces plus fencing, walls, and gates).

[a] In some cases.

- Instruction on best techniques should be provided; our analysis found that **multiple people tackling the shooter from multiple directions was consistently effective at ending attacks**.

On Armed Responses

Armed responses have been effective but are secondary to other physical responses (notably, tackling the shooter). Having an armed response depends on having an armed person with the necessary training to stop a shooter successfully; hence, most armed responses were carried out by security guards or on-scene officers, with only a few cases of armed bystanders doing so. As noted, armed responders have sometimes been ineffective, either not engaging (whether unable or unwilling) or being overpowered or shot. ST-CP bystanders and security personnel are unlikely to always have trained armed responders within range when an attacker strikes; therefore, unarmed security and bystanders should be ready to respond appropriately to an attack.

A Need to Improve the Utility of Surveillance

For those locations that warrant camera surveillance, the literature review and detailed case studies identified several issues:

- Placement of cameras should avoid leaving major blind spots.
- Cameras need to be actively monitored, either manually or with the assistance of video analytic tools that can detect the appearance of guns or gunshots.
- Cameras need to be maintained.

Issues Involving the Defenses of Secured Buildings

A Need for Site Plans to Put Distance, Movement, and Barriers Between Would-Be Attackers and Bystanders

A high-casualty attack typically occurs when a shooter takes a crowd by surprise (at once or over time in multiple rooms); in contrast, a shooter left to target people from outside or at great distances typically causes a low-fatality event. Thus, measures that disrupt an attacker's ability to surprise a crowd at close range are of high value. As noted in the mitigation section of the MADT, these include measures that put distance, movement, and barriers between attackers and bystanders, such as the following:

- Secure outer perimeter defenses (such as fencing, gates, and cameras) ideally keep attackers far outside the site, or at least provide the timeliest-possible warning. Security managers should assess the size of each site's defended perimeter to balance it being of sufficient size for the people within while limiting costs.
- Secure facility walkups and entry vestibules provide an opportunity to keep an attacker outside or bottled in an entryway.
- Secure locks, doors, and windows similarly keep attackers away from crowds.

- Pathways that lead bystanders to secure areas (which are secured against attackers) provide key distance and barriers against attackers.
- Sensors and alerting systems that provide early warning of a person with a gun—or shooting—can provide additional time for bystanders to secure themselves or escape and for security to respond.

A Need for Up-to-Date Active-Assailant Training That Minimizes Adverse Psychological Consequences

In the literature review, we noted that training is needed for building management, security, and bystanders in the building to use these capabilities effectively; this includes basics of active-assailant response plus awareness of what the site's active-assailant alerts sound like and what to immediately do and where to go when they go off. Some have expressed concern that active-shooter drills—especially more-realistic ones—can cause adverse mental health effects; training should focus on building knowledge, skills, and confidence rather than on realistic attack simulation.[9] The literature review and case studies also suggest posting flyers summarizing key reminders on what to do in the case of an attack, as well as on recognizing and reporting suspicious behavior.

A Need to Curtail Failures in Secured Doors and Windows, the Most-Critical and Most-Efficient Measures

Secured doors and windows that prevent would-be shooters from entering buildings—or, internally, from getting into spaces where crowds are present—were the measures with the most evidence of effectiveness and cost-efficiency. (Other access control measures, such as ID badges, were also reported as cost-effective.) However, there have been several notable failures of these measures, including in the Sandy Hook Elementary School shooting (the shooter shot through a large window next to the door); the Uvalde, Texas, elementary school shooting (the shooter was able to get through what should have been a locked external door); and the March 2023 Nashville Covenant School shooting (the shooter shot through external glass doors).[10] Doors and locks must be maintained, and windows must be secured. For large, accessible windows, security (or entry-resistant) film should be considered; although it does not make windows bulletproof, it does make them much harder to enter because the attacker must force their way through the plastic film. The Texas Education Agency recently required adding security film to ground-floor windows and glass doors.[11]

[9] For example, ElSherief et al., "Impacts of School Shooter Drills on the Psychological Well-Being of American K–12 School Communities."

[10] ABC News, "Tragedy at Sandy Hook"; Hollingsworth, "Unlocked Doors Were 'First Line of Defense' at Uvalde School"; Mascall and Hutchinson, "Nashville School Shooting Puts Renewed Focus on Doors, Security."

[11] Hattersley, "Texas Schools Must Install Window Security Film."

A Need for Updated Medical Supplies and Training, Especially on Bleeding

Medical standards for tactical care have been updated, both on stopping bleeding from those suffering gunshot (and other) injuries and in general.[12] Facility managers must maintain updated equipment and first aid training.

Issues Involving the Defenses of Major Venues

A Need to Avoid Creating Accessible Crowds Awaiting Entry into a Venue

Security screening measures that create large external crowds waiting to go into a venue create an accessible crowd for a would-be attacker.

A Need to Position Guards to Provide a Deterrent Effect

This was noted in the literature review and detailed case studies. Positioning guards for deterrence provides an additional value for guards beyond just direct response to attacks (or other security threats). To achieve this effect, the guards must be highly visible—notably, at major points of entry.

A Need to Support Security for Soft Targets and Crowded Places

As with protection measures, there is a general need to provide management, planning, training, and funding for ST-CP security measures. Security managers and plans have been identified as being some of the most cost-effective security measures.

Protection: Response Layers of Security

Figure 5.6 shows the response layers of security, which both stop the attack and provide medical treatment to minimize casualties as quickly as possible.

A Need to Improve the Initial Setup of Incident Command

As noted in the literature review, there have been frequent problems with initial stand-up of incident commands and assigning initial duties.

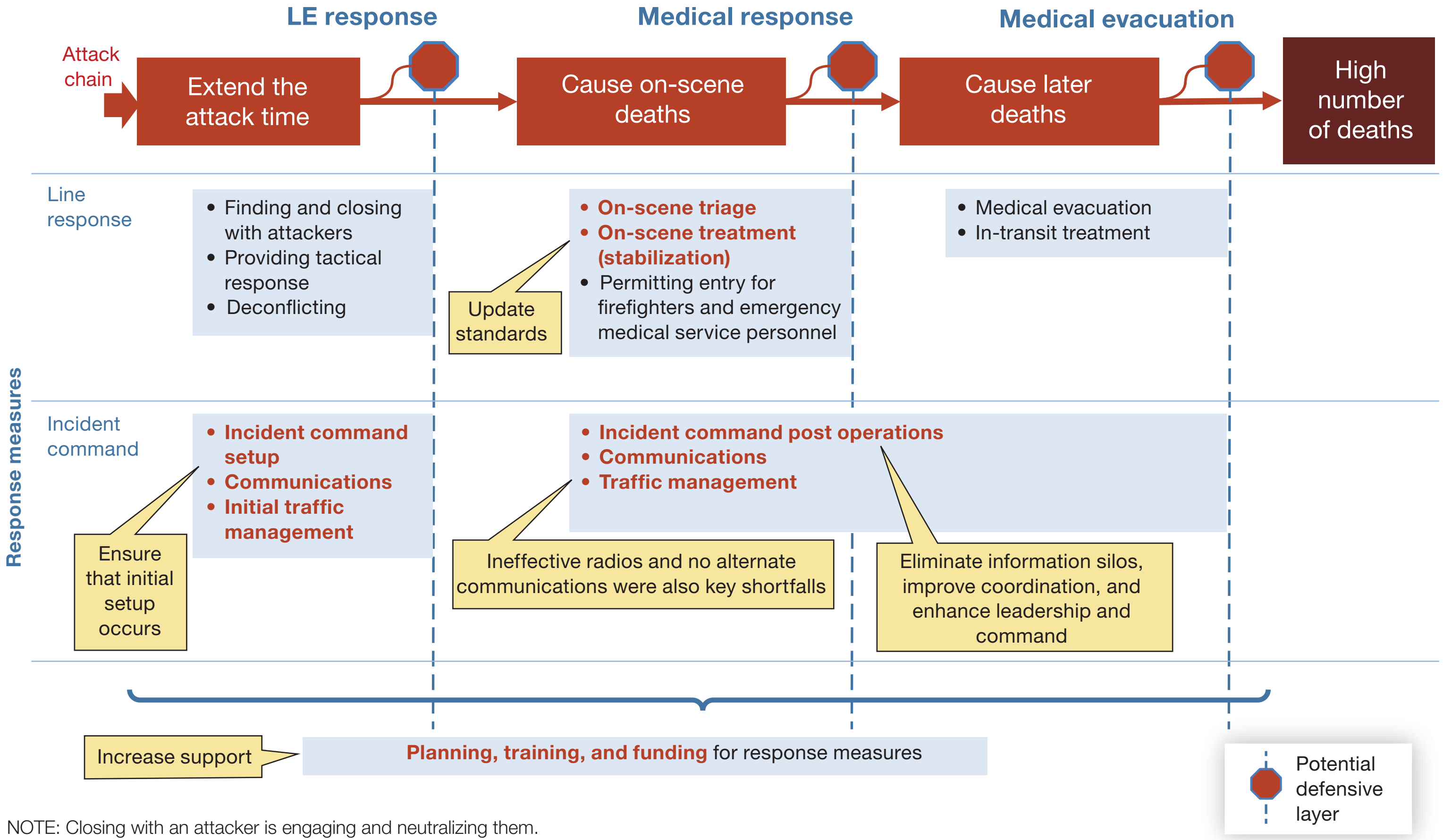
A Need to Improve Incident Command Post Operations More Broadly

As noted in the literature review, AARs have commonly noted a series of major command-and-control problems, including lack of clarity about roles (including what roles should be), problems dealing with influxes of responders, and, as a result, problems getting key respond-

[12] See American College of Surgeons, "Stop the Bleed," and Committee for Tactical Emergency Casualty Care, homepage.

FIGURE 5.6

Protection: Response Layers of Security and Related Issues



LE response
Medical response
Medical evacuation
Attack chain
Extend the attack time
Cause on-scene deaths
Cause later deaths
High number of deaths
Response measures
Line response
• Finding and closing with attackers
• Providing tactical response
• Deconflicting
• On-scene triage
• On-scene treatment (stabilization)
• Permitting entry for firefighters and emergency medical service personnel
Update standards
• Medical evacuation
• In-transit treatment
Incident command
• Incident command setup
• Communications
• Initial traffic management
Ensure that initial setup occurs
• Incident command post operations
• Communications
• Traffic management
Ineffective radios and no alternate communications were also key shortfalls
Eliminate information silos, improve coordination, and enhance leadership and command
Increase support
Planning, training, and funding for response measures
Potential defensive layer

NOTE: Closing with an attacker is engaging and neutralizing them.

ers into the site and treating and evacuating the injured in a timely manner. AARs have suggested, as remedies, following NIMS guidelines, having a common framework and language for command, establishing agreements on roles and chains of command, and conducting joint training events. Providing plans and schematics of major ST-CP venues, such as schools, houses of worship, malls, theaters, and stadiums, to responding agencies in advance was also noted as a measure that could expedite awareness and command.

A Need to Improve Communications from Both Technical and Operational Perspectives

The literature review noted many technical problems, including radio functioning, radio interoperability, and even a lack of charging equipment. The review also noted operational (doctrinal and procedural) issues, with overcrowded channels precluding getting situational awareness information even if radio systems were interoperable.

A Need for Improved Support for Multiagency Coordination, Planning, and Training

AARs have suggested, as remedies for command and communication issues, following NIMS guidelines, having a common framework and language for command, establishing agreements on roles and chains of command, and conducting joint training events. Providing plans and schematics of major ST-CP venues, such as schools, houses of worship, malls, theaters, and stadiums, to responding agencies in advance was also noted as a measure that could expedite awareness and command. All these planning and training measures, however, require support for implementation.

Overall Findings for All Layers of Security

This section presents findings about the system-based approach to ST-CP security from a holistic perspective. Figure 5.7 summarizes these high-level findings.

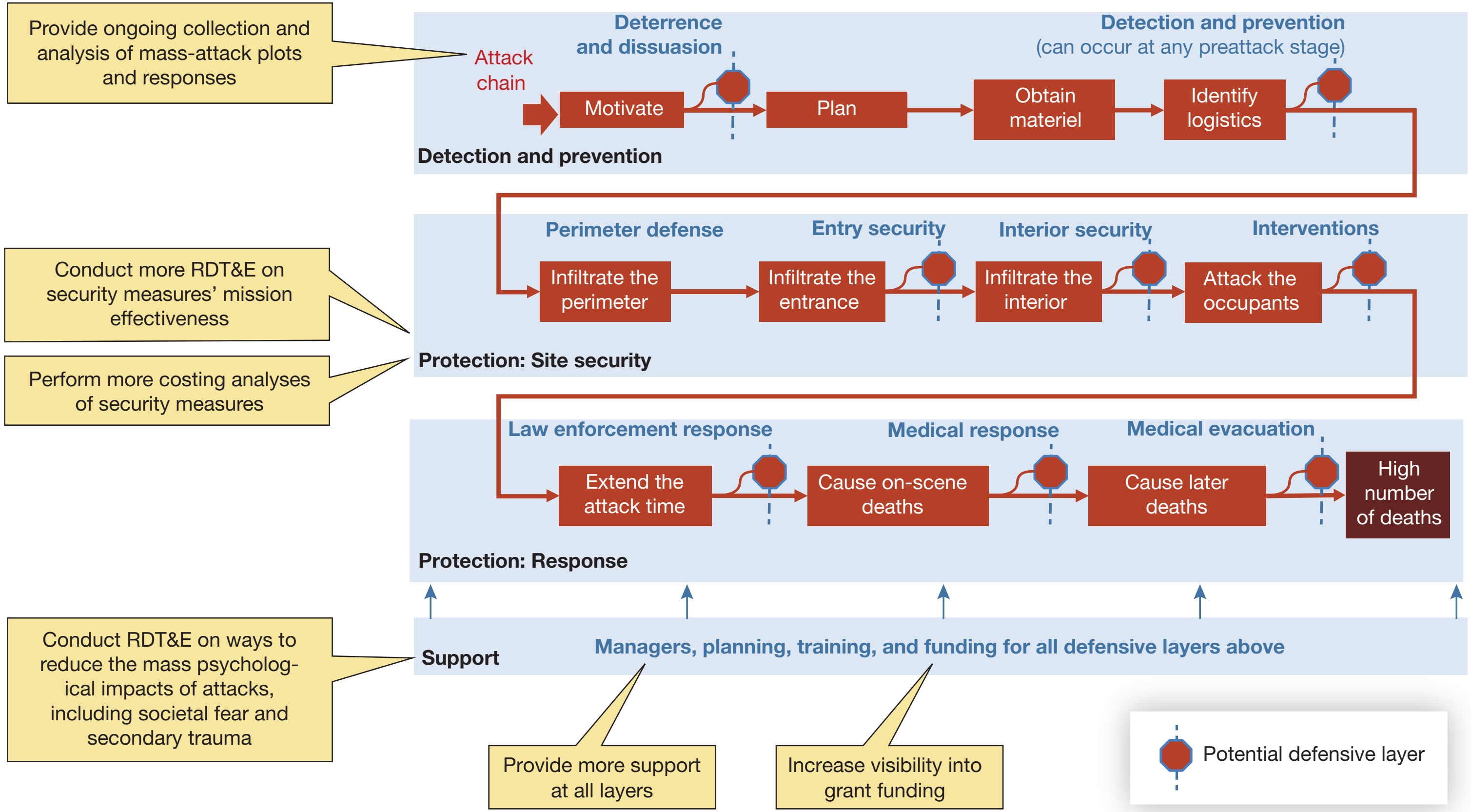
Data Collection and Analysis

A Need for Ongoing Collection and Analyses of Data on Mass-Attack Plots and Responses

Ongoing collection and analysis are especially key for foiled plots and failed plots (attacks that are stopped almost immediately before reaching targeted crowds) because data on these plots typically are less collected and studied. To help security partners adjust to any major developments or trends, there is also a need for rapid turnaround for data and analysis of recent plots.

FIGURE 5.7

General Issues in Mass-Attack Security


Provide ongoing collection and analysis of mass-attack plots and responses
Attack chain
Deterrence and dissuasion
Detection and prevention (can occur at any preattack stage)
Motivate
Plan
Obtain materiel
Identify logistics
Detection and prevention
Conduct more RDT&E on security measures' mission effectiveness
Perform more costing analyses of security measures
Perimeter defense
Entry security
Interior security
Interventions
Infiltrate the perimeter
Infiltrate the entrance
Infiltrate the interior
Attack the occupants
Protection: Site security
Law enforcement response
Medical response
Medical evacuation
Extend the attack time
Cause on-scene deaths
Cause later deaths
High number of deaths
Protection: Response
Conduct RDT&E on ways to reduce the mass psychological impacts of attacks, including societal fear and secondary trauma
Support
Managers, planning, training, and funding for all defensive layers above
Provide more support at all layers
Increase visibility into grant funding
Potential defensive layer

NOTE: Some ordinary criminal cases could qualify as mass attacks. Unintended social costs of security could be high, especially for schools and houses of worship.

A Need to Reevaluate Whether Ordinary Criminal Mass Shootings Should Be Considered Mass Attacks

In reviewing examples of mass shootings considered to be ordinary crime, we identified cases in which many bystanders (on the street or at a social event) were shot in addition to the intended targets, seemingly at random. It appears that some shooters were deliberately targeting uninvolved bystanders for personal reasons, as opposed (or in addition to) to carrying out targeted violence for criminal purposes, which means that some of the ordinary-crime mass shootings should be categorized as mass attacks on the public.

There is a need to assess high-casualty, ordinary-crime mass shootings to understand whether some of these should be considered mass attacks and thus given the same level of attention as other mass attacks. Some examples from 2023 include the June 2023 DuPage County, Illinois, shooting at a Juneteenth party (23 shot, one fatally) and the April 2023 Dadeville, Alabama, shooting at a birthday party (36 shot, four fatally).[13]

Evaluation of Security Measures

A Need for More Research, Development, Testing, and Evaluation on the Effectiveness of Security Measures

Although there is much testing to ensure that security products work as intended, we found few studies of whether security measures work to stop attackers under realistic conditions.

A Need for More Costing Analysis of Security Measures

Costing analyses of the efficiency of security measures would help security planners determine how to invest limited resources.

The Psychological Effects of Attacks and Security Measures

A Need to Reduce the Mass Psychological Impacts of Attacks

Saturation or immersive coverage of mass attacks has been speculated to be inducing secondary trauma and a great deal of fear of mass attacks, making people much more fearful of becoming victims themselves than statistics warrant. In addition, the impact on the public might motivate some would-be attackers who seek the fame that such coverage can bring to the perpetrator of a mass attack.

A Need to Reduce the Psychological Effects of Security Measures

As noted in the literature review, some studies have shown potential social and psychological costs of security (and the perceived threat), especially in places that people believe should especially be safe, such as schools and houses of worship. Active-assailant training, having

[13] Holpuch and Bubola, “23 Shot, 1 Fatally, at a Juneteenth Celebration in Illinois”; White, “Four Killed, 28 Injured in Dadeville Shooting.”

to go through metal detectors, and highly visible CCTV cameras have also been flagged as potentially causing adverse psychological consequences. Security measures need to be adapted to reduce the psychic costs of security.

This is a specific consideration for active-shooter training. Both the literature review and quantitative case analysis point to the importance of providing this training to those who will be in key ST-CP sites and the public; the issue is the need to do so in ways that minimize adverse effects.

Increasing Support to Security Layers

A Need for Visibility into Existing Grant Funding

The grant analysis identified billions of dollars in available funding for ST-CP security, along with detailed characterizations of entities that might be eligible, submission and administration requirements, and award criteria. However, the analysis also identified a lack of capability to monitor how ST-CP funds are being spent. There is a need to provide visibility into and transparency of ST-CP grant spending. Requiring the reporting of fine details could raise security concerns, but there should be at least categorical reporting.

A Need for Support for Management, Planning, and Training

Across layers and ST-CPs, there was a consistent need to provide support for the nonmateriel—management (and managers), planning, and training.

CHAPTER 6

Recommendations: A Road Map for Improving Prevention of and Protection from Attacks on Soft Targets and Crowded Places

This chapter presents the proposed *innovation road map*: candidate solutions to address the issues identified in the landscape assessment, along with relationships between them. We present proposals both for RDT&E and for funding priorities. Some of these proposals have been prioritized; these proposals generally apply to cases in which a capability gap needs to be addressed with not so much done to date to address it.

Research, Development, Testing, and Evaluation Efforts

The following suggested types of studies should broadly follow an RDT&E process, including R&D incorporating involvement from multiple types of experts and stakeholders, initial testing, and evaluations of field pilots. Figure 6.1 shows this sample process.

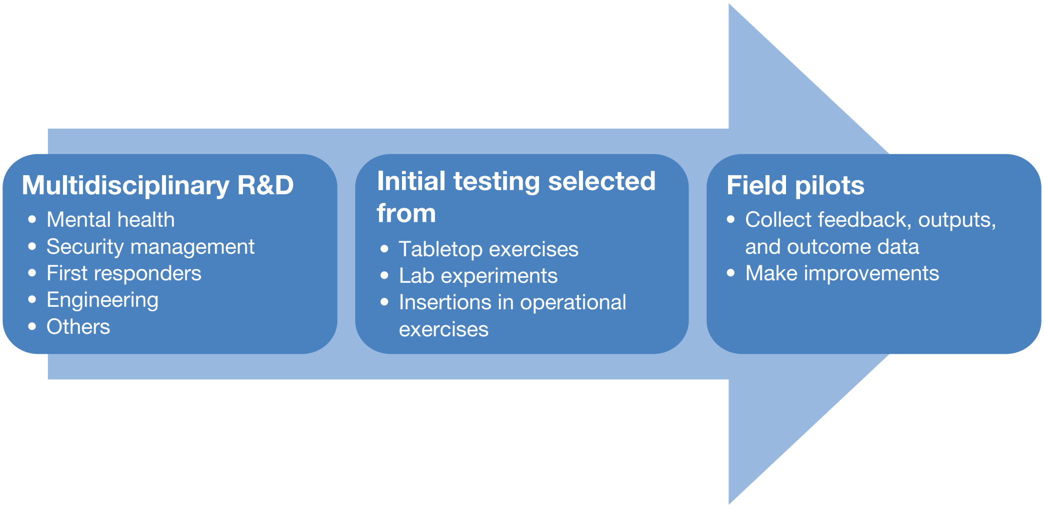
Improving Prevention: Countermotivation

Seek Methods for Deterring and Dissuading Would-Be Attackers

Studies in this area should focus on persuading would-be attackers—or those considering committing to attacks—to cease plans altogether. These studies should incorporate effects of today's ST-CP security measures; however, the focus should go beyond just discouraging an attacker from hitting a specific target, which can lead them to choose more-vulnerable targets. They should also counter the current social validation of shootings that would-be attackers can experience online.[1] Given the increases in mass-shooting attacks and plots, finding ways to reduce intentions to attack is a critical need.

[1] Peterson and Densley, "Reflections on Researching the Lives and Crimes of Mass Shooters."

FIGURE 6.1
Sample Research, Development, Testing, and Evaluation Process for Efforts to Develop Security for Soft Targets and Crowded Places



Multidisciplinary R&D

- Mental health
- Security management
- First responders
- Engineering
- Others

Initial testing selected from

- Tabletop exercises
- Lab experiments
- Insertions in operational exercises

Field pilots

- Collect feedback, outputs, and outcome data
- Make improvements

Improving Prevention: Detection and Reporting

Develop Indicators of and Education About Suspicious Seeking of Weapons

We recommend that researchers work directly with gun advocates and gun industry representatives because they are likeliest to know what types of actions are genuinely suspicious. We also recommend that these efforts cover suspicious acquisition of ammunition in addition to acquisition of weapons; as noted, there can be cases in which someone has ready access to a firearm but not to hundreds or thousands of rounds of ammunition and corresponding clips. Given the general shortfalls in detecting concerning weapon acquisition, this appears to be a major opportunity to strengthen ST-CP attack prevention and is a critical need.

Enhance "See Something, Say Something" Campaigns

We recommend providing additional insight into both what to look for and how to report it, especially for those who are concerned but do not think those concerns warrant calling 911. As noted, these should include assurances that, except in extreme situations, those reported will not face charges.[2]

Develop and Evaluate Campaigns to Reduce Threats of Violence—Most Notably, Online and by Students

As noted, there have been recent concerns that threat assessment resources are being overwhelmed by false threats to carry out mass shootings. Existing campaigns provide both

[2] Interviewees in the MADT project said that they tried hard not to arrest anyone until the person had made arrangements to the point at which an attack appeared inevitable (and usually imminent).

examples and opportunities for evaluation to see how well the campaigns are working and what might be done to improve them.[3] In conducting these campaigns, it will be important to reconcile the threat (and actuality) of punishment for deterrence with persuading bystanders that it is fine to report because the subject's life will not be ruined.

Improving Prevention: Assessment

Develop Technical Rules and Processes for Assessment, Monitoring, and Follow-Up

Although much work has been done in this area, not much has been done on developing formal quantitative rules and business processes. Here, formal rules might include point-scoring rubrics or decision trees to take the presence or absence of indicators and advise what to do next. Existing indicators, plus data assessing how indicative they are in practice, can provide inputs to developing these rules. Here, "how indicative" needs to account for both false positives and false-negative issues and ensure that the resulting rules have similar results across demographic lines. Past cases can be used to check alignment as well.

Improving Prevention: Interventions

Develop Protocols and Education for Wellness Checks

We recommend working with mental health and LE personnel with prior experience conducting wellness checks to develop these protocols. Given the importance of wellness checks in prevention and the general lack of formal protocols, this is a critical need.

Improving Protection: General Site Protective Measures

Evaluate the Effectiveness and Cost-Effectiveness of Security Measures More

We identified few studies examining the effectiveness or cost-effectiveness of security measures in stopping active shooters and other types of mass attacks. (This is in contrast to general discussions and guidance on security measures, as well as evaluations to test whether equipment works in line with standards and specifications.) The major exceptions were for access control measures and security managers.

The comparative rarity of mass attacks makes it difficult to assess specific technologies based on past performance. We envision lab and exercise testing against simulated attackers, including control and experimental runs, under conditions ranging from "defenders advan-

[3] FBI, "Think Before You Post"; Miami-Dade County Public Schools, "It's No Joke."

taged" to "attacker(s) highly advantaged." Alignment of products and nonmateriel measures with past attacks, plus performance with security proxies,[4] can also be analyzed.

According to our landscape-assessment results, topics should include studies on placement and monitoring of access controls, cameras, and shot sensors; studies on the effectiveness of sensor and analysis systems intended to detect weapons or other kinds of attacks from greater standoff distances; and screening systems, including new walk-through-at-speed systems. In general, our interviewees noted growing trends of attempting to incorporate AI technologies into security systems; a growing number of evaluations will likely be needed for AI-inside technologies in coming years. Given the importance of and large expenditures for security measures, this is a critical need.

Conduct More Studies on the Social Costs of Security Measures and Mitigations, Especially for Schools and Houses of Worship

As noted in the earlier discussion, some have expressed concerns about the social and psychological costs that security measures are having, especially in places that are commonly perceived as places that should be especially safe and open, such as schools and houses of worship. The recommended studies should focus not just on characterizing effects but also on how to tailor security measures to minimize their psychological and social impacts. This notably includes reducing the impact of (and seeking alternatives to) active-shooter drills.

Improving Protection: Security for Open and Nonsecure Spaces

Develop a Model Concept of Operations for Open and Nonsecure Spaces, Such as Shopping Malls and Restaurants

Although bystanders in open spaces have the advantage of being able to flee more readily than those in other venues, most of the traditional security measures, including doors, locks, and guards, are generally absent in open spaces. The few constant elements are generally bystanders and their cell phones. Other security measures, including the presence of barriers, entry points, guards, or surveillance, are expected to be present intermittently. There is a need for concepts of operations (CONOPSs) for open and nonsecure spaces that

- leverage what bystanders and their cell phones might do
- leverage what security measures a given ST-CP site has present, tailored to those measures
- assist in prioritizing which security measures to add that would most increase security while maintaining an open characterization, given limited resources.

[4] Proxies are incidents that have some similarities with mass attacks but are much more common. For example, technologies designed to prevent people from getting into a building can be assessed against numbers of general break-ins, including for ordinary criminal purposes.

Given the numbers of attacks that take place at open and nonsecure sites, as well as the fact that most studies to date have focused on secure buildings, this is a critical need.

Improving Protection: Improving Attack Response

Continue to Seek Improvements to and Develop Training Packages on Command and Control, Leadership, and Coordination

This requires paying attention to the specific deficiencies pointed out in AARs.

Study Alternatives to Traditional Voice Radio Communications

These include preemptive fourth-generation (4G) and fifth-generation (5G) wireless communications that are not restricted to push-to-talk technology, text message–based applications and concepts, and situational awareness displays and tools that limit the need for voice communications asking for situational updates. Over time, these will need to supplant (or at least augment) traditional push-to-talk communications as primary communication modes for most operations.

Improving Defenses for Soft Targets and Crowded Places in General: Studies on the Overall Scope of Mass Attacks

Continuously Track and Analyze Mass-Attack Plots

An ongoing effort is needed to collect and analyze data on plots (foiled and executed), as close to the time they are exposed as possible, to detect meaningful changes and trends.

We also recommend considering survey research to estimate and characterize the size of the gray area—threat assessments that do not end in a public arrest but in which the assessment team believed there was some potential for a subject to escalate to violence. Given the importance of maintaining awareness of the most-recent trends in mass attacks, this is a critical need.

Review Mass-Shooting Events to Determine Whether Some Ordinary Criminal Shootings Should Be Treated as Mass Attacks on Soft Targets or Crowded Places

This review should start with high-casualty criminal mass-shooting cases in which large numbers of uninvolved bystanders were shot. In some cases, a shooter might have been targeting the uninvolved bystanders deliberately for personal reasons instead of (or in addition to) targeted violence for criminal purposes, meaning that those cases should be treated as ST-CP mass attacks. Given the magnitude of the attacks and resulting victimization, which might need additional scrutiny, this is a critical need.

Seek Ways to Reduce the Mass Psychological Impacts of Attacks, Including Societal Fear and Secondary Trauma

The social and psychological impacts of mass attacks have been enormous and are further believed to have helped inspire would-be attackers. These might cover potential public health campaigns at both macro and micro levels, along with potential changes to immersive, saturation coverage of shootings. Given the impacts, as well as the potential incentives for attackers, reducing these impacts is a critical need.

Funding and Policy Priorities

In general, we have three recommendations pertaining to funding and policy priorities:

- **Focus on the basics**, such as provision and maintenance of access control equipment and public education campaigns on what to look for and how to report it.
- **Seek to strengthen the system-based, layered security framework**, funding improvements to layers of security in ways that reinforce each other.
- **Funding and policy priorities should reflect RDT&E findings** as they become available.

Grant Management Priorities

We could not find much information about how grants for ST-CP prevention and protection are spent, other than basic topics and overall budget requirements.

Ensure That Grant Solicitations Include Tracking Requirements

Grants for ST-CP prevention and protection should be packaged with requirements to include budgets listing new personnel, items, and services for ST-CP planned for purchase (if not already required), as well as planned outputs and outcomes (explaining what the requested personnel, products, and services are intended to accomplish). They should also include requirements for regular reporting using a specified framework, helping ensure that funds for ST-CP security are being spent as intended.

Have Ongoing Disclosure and Monitoring

Grants should come with requirements for ongoing disclosure and monitoring to ensure alignment with priorities, starting with making ST-CP–related budget requests (or at least nonsensitive extracts of them) readily available.

Prevention Priorities

Fund Enhanced Public Education and Training on What to Report and How

Education and training should build on "see something, say something" principles and similar initiatives. Education and training should include working with social media companies to improve readiness of reporting violent threats and other potential plot information over social media channels. This effort can also include programs to educate the public on the importance of reducing hoax and other false threats. This effort would be informed by the RDT&E efforts to develop indicators (e.g., suspicious procurement of weapons), enhanced public education programs, and enhanced efforts to reduce the number of false threats. Given the centrality of public reporting to preventing attacks, this is a critical priority.

Provide Additional Funding to Cross-Organizational Threat Assessment Teams and Managers

To improve efficiency, this can cover threats besides mass attacks. As noted in the landscape assessment, fusion centers can and should be leveraged to support these teams as needed. This effort would be informed by the RDT&E effort to develop formalized threat assessment analysis rubrics and processes. Given the centrality of assessing and acting on tips from the public and other sources to prevention, this is a critical priority.

Protection Priorities: On-Site Security

Fund Enhanced Public Education and Training on How to Respond to an Active Attacker

Education and training on how to respond to an active attacker builds on "run, hide, and fight" principles. According to what we found in the landscape assessment, such training should include the following:

- "Run" needs to include flight to areas secured away from attackers, not just "outside."
- "Hide" needs to be genuinely hidden—ideally, in an area locked away from a shooter. This should not include hiding under desks, under tables, or around walls or bookcases in ready view of a shooter.
- "Fight" is mandatory if in close line of sight to a shooter. Tackling the shooter from multiple directions while avoiding charging straight at them is the best approach; throwing objects at or around shooters also has some value in distracting them. (One expert suggested labeling this approach as "Surround. Distract. Attack from the Back.") In general, there is a need to train bystanders to respond to active attackers the same way they would respond to someone trying to hijack a plane post-9/11.

Given the centrality of bystander actions in reducing casualties, this is a critical priority.

Provide Additional Funding to Cross-Organizational Security Teams and Managers

As with threat assessment teams, additional funding can cover threats besides mass attacks to improve efficiency. The security teams would be informed by the RDT&E findings on security measures' effectiveness and efficiency, updated site security guidance, and training (see the next recommendation). Depending on their responsibilities, they might also be informed by the open-space security CONOPS RDT&E. Given the centrality of site security managers and teams to reducing casualties and successful response, this is a critical priority.

Fund and Distribute Updates of Site Security Guidance Documents and Training

Site security guide documents should be regularly updated in response to changes and trends in attacks (as tracked by the ongoing RDT&E to monitor plots) and cover site security updates described in the landscape-assessment floor plan discussion in particular.

As discussed, in general, site management plans—including floor plans—should reflect having defensible and delayable entries and capabilities to secure interior portions from attackers; they should also avoid generating accessible crowds waiting to enter the site. Given the centrality of site management plans and keeping them up to date, this is a critical priority.

Fund Access Control Systems

Funding access control systems is especially important for the basics of procurement and maintenance of locks, doors, windows, and security film for accessible glass windows and doors. Given the effectiveness and comparatively low cost of access control systems, this is a critical priority.

Fund Increases in Mass-Attack Incident Training

Mass-attack incident training includes tabletop events, at a minimum, along with exercises for major, high-risk sites or regions. These should be integrated with training for first responders (see the next recommendation). Incident training should be updated in response to RDT&E findings about trends in attacks, as well as findings on security measures that are most effective and efficient.

Fund Additional Medical Supplies and Training

As noted, medical supplies and training should reflect "Stop the Bleed" and Committee for Tactical Emergency Casualty Care standards.

Protection Priorities: Response

Fund Supplies for First Responders Matching Updated Medical Standards

As noted, medical supplies and training should reflect "Stop the Bleed" and Committee for Tactical Emergency Casualty Care standards, which are more detailed for medical responders than for bystanders or LE.

Fund Additional Mass-Attack Incident Training

Additional training includes tabletop events along with exercises for major, high-risk sites or regions. These should be integrated with training for site security managers and teams (see earlier recommendations). Incident training should be updated in response to RDT&E efforts to improve command-and-control models, as well as improved communications and situational awareness tools.

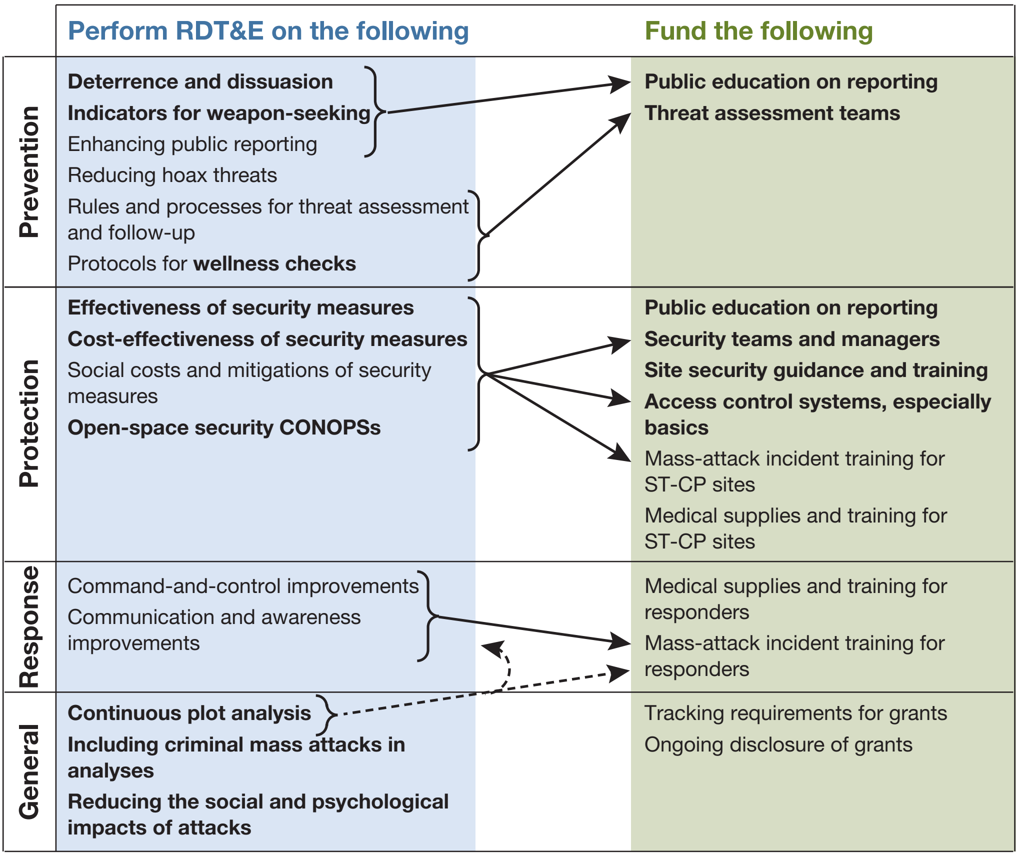
In Conclusion: A Summary of the Road Map

Figure 6.2 summarizes the principal RDT&E and investment recommendations. It also identifies the key interactions between them, as described in this chapter. These interactions include showing, notably, how RDT&E results should inform certain funding initiatives. As shown, the prevention RDT&E findings will inform both public education on reporting and the work of threat assessment teams. Similarly, site protection RDT&E findings will inform ST-CP site security teams, guidance, and event training, and response RDT&E findings will inform mass-attack training for first responders. Of note is that the ongoing analyses of discovered plots should directly inform ongoing RDT&E and funding initiatives because all will need to be updated to reflect changes in attack patterns and trends.

Overall, the United States has already made substantial progress in reducing the threat of ST-CP attacks by, for example, preventing a strong majority of plots. As shown by this road map, there are substantial opportunities to improve defenses further.

FIGURE 6.2

Summary of the Prevention and Protection Road Map for Soft Targets and Crowded Places



	Perform RDT&E on the following	Fund the following
Prevention	**Deterrence and dissuasion** **Indicators for weapon-seeking** Enhancing public reporting Reducing hoax threats Rules and processes for threat assessment and follow-up Protocols for **wellness checks**	**Public education on reporting** **Threat assessment teams**
Protection	**Effectiveness of security measures** **Cost-effectiveness of security measures** Social costs and mitigations of security measures **Open-space security CONOPSs**	**Public education on reporting** **Security teams and managers** **Site security guidance and training** **Access control systems, especially basics** Mass-attack incident training for ST-CP sites Medical supplies and training for ST-CP sites
Response	Command-and-control improvements Communication and awareness improvements	Medical supplies and training for responders Mass-attack incident training for responders
General	**Continuous plot analysis** **Including criminal mass attacks in analyses** **Reducing the social and psychological impacts of attacks**	Tracking requirements for grants Ongoing disclosure of grants

NOTE: Bold indicates a recommendation of critical importance. Plot analyses inform most ongoing RDT&E and funding recommendations. A solid arrow indicates that findings from the RDT&E on the left should inform the funding decision on the right. Because no RDT&E is needed to inform funding of medical supplies, no arrow is needed there. The dashed arrows indicate that continuous plot analysis should inform virtually everything else.

APPENDIX

Interview Protocol

For this report, we interviewed several types of stakeholders in the ST-CP security enterprise. These included state- and local-level LE and intelligence professionals, security industry representatives, venue security managers, representatives of civil society, and privacy advocates with stakes in improving ST-CP security. The team developed a general topic list that guided the discussion and specific questions relevant to the stakeholder's role in ST-CP security. These are presented in this appendix.

General Topics

- How has spending on ST-CPs security changed in the past 30 years?
- How have incidents changed over that time (frequency, lethality, threat actor)?
- What factors affect the number, lethality, or type of threat actors responsible for attacks on ST-CP targets?
- What opportunities (programs, policies, technology) do people see for reducing the number or lethality of incidents?
- What are the unintended consequences (positive and negative) of increased ST-CP security?
- How do ST-CP priorities align with factors affecting the frequency and lethality of incidents? Are there any significant gaps or shortfalls?
- How do ST-CP attacks' frequency and lethality vary by geographic region?
- How are AI technologies affecting ST-CP security measures?

Specific Stakeholder Questions

Government Security Professionals

- For what specific programs is your agency responsible for ST-CP defense?
- How does your agency interact with SLTTs or private industry?
- How has the ST-CP threat changed?
  - threat actors
  - frequency

  - targets
  - lethality
- Does your agency spend money on ST-CP prevention, protection, and response?
  - Types of spending (training, equipment, personnel, etc. . . .)
  - How is spending determined?
  - What kinds of projects have been funded?
  - How has spending changed in the past ten years?

Other Security Professionals (Industry Security Professionals, Technology Experts, Insurance Experts)

- What type of threats are you most concerned with?
- What type of interactions do you have with federal or SLTT agencies?
  - What federal or SLTT security products do you use?
- What types of general protective measures are employed at your sites?
- What is your process (risk assessment) for determining the proper level of protection for your site?
- How have implemented security measures affected your site's operations?
- What developments in security, in your experience, have been most effective (or at least most promising) in recent years? What have been the biggest disappointments?

Civil Society Experts (Privacy and Civil Right Experts)

- How has new technology affected privacy or civil rights concerns?
  - What technologies or security measures are most concerning?
- What are the unintended consequences (positive and negative) of increased ST-CP security?
- How are concerns expressed to government or industry officials?

Abbreviations

9/11	September 11, 2001
AAR	after-action report
AI	artificial intelligence
ALERT	Advanced Law Enforcement Rapid Response Training Center at Texas State University
CCTV	closed-circuit television
CISA	Cybersecurity and Infrastructure Security Agency
CONOPS	concept of operations
CP	crowded place
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FY	fiscal year
HSGP	Homeland Security Grant Program
HSOAC	Homeland Security Operational Analysis Center
ID	identification
IES	Institute of Education Sciences
IPR	intercity passenger rail
K–12	kindergarten through grade 12
LE	law enforcement
MADT	Mass Attacks Defense Toolkit
MSDHS	Marjory Stoneman Douglas High School
N/A	not applicable
NAICS	North American Industry Classification System
NCES	National Center for Education Statistics
NIJ	National Institute of Justice
NIMS	National Incident Management System
NPSG	Nonprofit Security Grant Program
NSGP-S	Nonprofit Security Grant Program—State
NSGP-UA	Nonprofit Security Grant Program—Urban Area
NTAC	National Threat Assessment Center
OPSG	Operation Stonegarden

PA	public address
PSGP	Port Security Grant Program
R&D	research and development
RDT&E	research, development, testing, and evaluation
SCP	situational crime prevention
SHSP	State Homeland Security Program
SLTT	state, local, tribal, or territorial
SME	subject-matter expert
SRO	school resource officer
ST	soft target
ST-CP	soft target or crowded place
THSGP	Tribal Homeland Security Grant Program
TSGP	Transit Security Grant Program
UASI	Urban Area Security Initiative
USSS	U.S. Secret Service

References

ABC News, "Tragedy at Sandy Hook," webpage, undated. As of June 21, 2023: https://abcnews.go.com/US/fullpage/newtown-ct-shooting-timeline-sandy-hook-elementary-school-18014080

Abrams, Zara, "Stress of Mass Shootings Causing Cascade of Collective Traumas," *Monitor on Psychology*, Vol. 53, No. 6, last updated September 1, 2022.

Addington, Lynn A., "Cops and Cameras: Public School Security as a Policy Response to Columbine," *American Behavioral Scientist*, Vol. 52, No. 10, June 2009.

American College of Surgeons, "Stop the Bleed," webpage, undated. As of June 23, 2023: https://www.stopthebleed.org/

Ancliffe, Simon, "Crowd Planning for Public Safety," *Perspectives in Public Health*, Vol. 137, No. 1, January 2017.

Arnold, Christopher, and Mary Ann Lasch, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*, U.S. Department of Homeland Security, Federal Emergency Management Agency 430, December 2007.

Arteaga, Cristian, and JeeWoong Park, "Building Design and Its Effect on Evacuation Efficiency and Casualty Levels During an Indoor Active Shooter Incident," *Safety Science*, Vol. 127, July 2020.

ASIS International, *Physical Asset Protection*, Standard ASIS PAP-2021, 2021.

ASIS International, *Protection of Assets: Physical Security*, 2021 ed., 2021.

Bachman, Ronet, Antonia Randolph, and Bethany L. Brown, "Predicting Perceptions of Fear at School and Going to and from School for African American and White Students: The Effects of School Security Measures," *Youth and Society,* Vol. 43, No. 2, June 2011.

Basner, Dave, "If You Hear a 'Code Brown' While Shopping, Get Out of the Store Immediately," iHeart, August 26, 2022.

Bigda, Kristin, "Strategies for Crowd Management Safety," *NFPA Today*, May 20, 2021.

Bohorquez, Juan Camilo, Sean Gourley, Alexander R. Dixon, Michael Spagat, and Neil F. Johnson, "Common Ecology Quantifies Human Insurgency," *Nature*, Vol. 462, No. 7275, 2009.

Braziel, Rick, Frank Straub, George Watson, and Rod Hoops, *Bringing Calm to Chaos: A Critical Incident Review of the San Bernardino Public Safety Response to the December 2, 2015 Terrorist Shooting Incident at the Inland Regional Center*, Critical Response Initiative, Office of Community Oriented Policing Services, U.S. Department of Justice, 2016.

Brenan, Megan, "Nearly Half in U.S. Fear Being the Victim of a Mass Shooting," Gallup, September 10, 2019.

Briggs, Thomas W., and William G. Kennedy, "Active Shooter: An Agent-Based Model of Unarmed Resistance," *Journal of Threat Assessment and Management*, Vol. 6, No. 3–4, 2019.

Broward County Aviation Department, *Fort Lauderdale–Hollywood International Airport Active Shooter Incident and Post-Event Response January 6, 2017: After-Action Report*, August 15, 2017.

Cerezo, Ana, "CCTV and Crime Displacement: A Quasi-Experimental Evaluation," *European Journal of Criminology*, Vol. 10, No. 2, 2013.

Chavez, Nicole, “A Family Wounded in the El Paso Massacre Is Suing Walmart over Lack of Security,” CNN, September 4, 2019.

Chief of Naval Operations, Department of the Navy, “Investigation into Fatal Shooting Incident on Naval Air Station Pensacola of 6 December 2019,” memorandum to Secretary of the Navy, July 7, 2020.

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Clark County Fire Department, Las Vegas Metropolitan Police Department, and National Exercise Division, Federal Emergency Management Agency, U.S. Department of Homeland Security, *1 October After-Action Report*, August 24, 2018.

Coaffee, Jon, “Rings of Steel, Rings of Concrete and Rings of Confidence: Designing out Terrorism in Central London Pre and Post September 11th,” *International Journal of Urban and Regional Research*, Vol. 28, No. 1, March 2004.

Committee for Tactical Emergency Casualty Care, homepage, undated. As of June 23, 2023: https://www.c-tecc.org/

Conley, Tom M., “Why the El Paso Massacre Was a Security Failure,” *Security Magazine*, August 26, 2019.

Connecticut State Police, *After Action Report: Newtown Shooting Incident December 14, 2012*, circa January 2018.

Connors, Edward, *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement*, Office of Community Oriented Policing Services, U.S. Department of Justice, March 2007.

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, *Security of Soft Targets and Crowded Places: Resource Guide*, April 2019.

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, *Mitigating Attacks on Houses of Worship: Security Guide*, December 2020.

Dalgaard-Nielsen, Anja, Jesper Laisen, and Charlotte Wandorf, “Visible Counterterrorism Measures in Urban Spaces: Fear-Inducing or Not?” *Terrorism and Political Violence*, Vol. 28, No. 4, 2016.

Devlin, Deanna N., and Denise C. Gottfredson, “The Roles of Police Officers in Schools: Effects on the Recording and Reporting of Crime,” *Youth Violence and Juvenile Justice*, Vol. 16, No. 2, April 2018.

DHS—*See* U.S. Department of Homeland Security.

Doherty, Erin, “Poll: 4 in 10 Americans Fear Being a Victim of Gun Violence,” Axios, August 23, 2022.

Doornbos, Caitlin, Christal Hayes, David Harris, and Gal Tziperman Lotan, “New Pulse Review from Orlando Police Reveals Details, Lessons Learned,” *Orlando Sentinel*, April 13, 2017.

Dorn, Michael, Sonayia Shepherd, Tina S. Brookes, Russell Bentley, Rod Ellis, William Miller, Chris Dorn, Tod Schneider, Steve Satterly, Phuong Nguyen, Ulric Bellaire, and Rachel Wilson, *Post-Incident Review: Arapahoe High School Active-Shooter Incident*, Safe Havens International, January 13, 2016.

Doss, Kevin T., and C. David Shepherd, *Active Shooter: Preparing for and Responding to a Growing Threat*, Elsevier, 2015.

Ducharme, Jamie, “A Third of Americans Avoid Certain Places Because They Fear Mass Shootings,” *Time*, August 15, 2019.

ElSherief, Mai, Koustuv Saha, Pranshu Gupta, Shrija Mishra, Jordyn Seybolt, Jiajia Xie, Megan O’Toole, Sarah Burd-Sharps, and Munmun De Choudhury, “Impacts of School Shooter Drills on the Psychological Well-Being of American K–12 School Communities: A Social Media Study,” *Humanities and Social Sciences Communications*, Vol. 8, 2021.

FBI—*See* Federal Bureau of Investigation.

FBI and ALERT—*See* Federal Bureau of Investigation and Advanced Law Enforcement Rapid Response Training Center at Texas State University.

Federal Aviation Administration, U.S. Department of Transportation, “Airport Improvement Program (AIP),” webpage, last updated June 27, 2023. As of June 27, 2023:
https://www.faa.gov/airports/aip

Federal Bureau of Investigation, U.S. Department of Justice, “Think Before You Post: Hoax Threats Are Serious Federal Crimes,” October 5, 2018.

Federal Bureau of Investigation, U.S. Department of Justice, *Active Shooter Incidents: 20-Year Review, 2000–2019*, May 2021.

Federal Bureau of Investigation, U.S. Department of Justice, and Advanced Law Enforcement Rapid Response Training Center at Texas State University, *Active Shooter Incidents in the United States in 2020*, July 2021.

Federal Bureau of Investigation, U.S. Department of Justice, and Advanced Law Enforcement Rapid Response Training Center at Texas State University, *Active Shooter Incidents in the United States in 2021*, May 2022.

Federal Bureau of Investigation, U.S. Department of Justice, and Advanced Law Enforcement Rapid Response Training Center at Texas State University, *Active Shooter Incidents in the United States in 2022*, April 2023.

Federal Emergency Management Agency, U.S. Department of Homeland Security, “FY 2023 Port Security Grant Program Fact Sheet,” February 27, 2023.

Federal Emergency Management Agency, U.S. Department of Homeland Security, “National Incident Management System,” webpage, last updated July 14, 2023. As of May 25, 2023:
https://www.fema.gov/emergency-managers/nims

Federal Emergency Management Agency, U.S. Department of Homeland Security, “Homeland Security Grant Program,” webpage, last updated September 5, 2023. As of December 9, 2023:
https://www.fema.gov/grants/preparedness/homeland-security

Federal Transit Administration, U.S. Department of Transportation, “Capital Investment Grants Program,” webpage, undated. As of June 27, 2023:
https://www.transit.dot.gov/CIG

FEMA—*See* Federal Emergency Management Agency.

Filardo, Mary, *State of Our Schools: America’s K–12 Facilities 2016*, 21st Century School Fund, 2016.

Fox, James Alan, and Jenna Savage, “Mass Murder Goes to College: An Examination of Changes on College Campuses Following Virginia Tech,” *American Behavioral Scientist*, Vol. 52, No. 10, June 2009.

Freilich, Joshua D., Jeff Gruenewald, and Marissa Mandala, “Situational Crime Prevention and Terrorism: An Assessment of 10 Years of Research,” *Criminal Justice Policy Review*, Vol. 30, No. 9, December 2019.

Freilich, Joshua D., and Graeme R. Newman, “Situational Crime Prevention,” in Henry N. Pontell, ed., *Oxford Research Encyclopedia of Criminology and Criminal Justice*, Oxford University Press, 2017.

Garrison, Joey, Chris Woodyard, Olivia Sanchez, and Samuel Gaytan, “At Least 20 Dead, 26 Wounded, Lone Suspect in Custody After Rampage at El Paso Walmart,” *USA Today*, August 3, 2019.

Gartenstein-Ross, Daveed, and Tadd Lahnert, “Crisis Architecture: Building to Defend Against Active Aggressors,” *War on the Rocks*, December 2, 2019.

Gastic, Billie, “Metal Detectors and Feeling Safe at School,” *Education and Urban Society*, Vol. 43, No. 4, 2011.

Global Programme on Countering Terrorist Threats Against Vulnerable Targets, United Nations Office of Counter-Terrorism, *Protecting Vulnerable Targets from Terrorist Attacks: Good Practices Guide—Introduction*, 2022.

Graf, Nikki, “A Majority of U.S. Teens Fear a Shooting Could Happen at Their School, and Most Parents Share Their Concern,” Pew Research Center, April 18, 2018.

Grant Programs Directorate, Federal Emergency Management Agency, U.S. Department of Homeland Security, “The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Tribal Homeland Security Grant Program,” May 13, 2022.

Grant Programs Directorate, Federal Emergency Management Agency, U.S. Department of Homeland Security, “The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program,” February 27, 2023.

Grant Programs Directorate, Federal Emergency Management Agency, U.S. Department of Homeland Security, “The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Intercity Bus Security Grant Program,” February 27, 2023.

Grant Programs Directorate, Federal Emergency Management Agency, U.S. Department of Homeland Security, “The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Nonprofit Security Grant Program,” February 27, 2023.

Grant Programs Directorate, Federal Emergency Management Agency, U.S. Department of Homeland Security, “The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Transit Security Grant Program,” February 27, 2023.

Grants Office, homepage, undated. As of October 12, 2023:
https://www.publicsafetygrants.info

Grants Office, “Grant Details: Intercity Passenger Rail (IPR) Program,” webpage, undated. As of June 27, 2023:
https://www.publicsafetygrants.info/Grant-Details/gid/14856

Gundry, Craig, “Physical Security Design and the Active Shooter,” Critical Information Services, March 17, 2020.

Hanover Research, *Best Practices in School Security*, March 2013.

Hattersley, Robin, "Texas Schools Must Install Window Security Film," *Campus Safety*, February 16, 2023.

Healthcare and Public Health Sector Coordinating Council, *Active Shooter Planning and Response: Learn How to Survive a Shooting Event in a Healthcare Setting*, updated January 24, 2017.

Healthcare and Public Health Sector Coordinating Councils Public Private Partnership, *Active Shooter Planning and Response in a Healthcare Setting*, January 2014.

Hennessy-Fiske, Molly, Jenny Jarvie, and Del Quentin Wilber, "Orlando Gunman Had Used Gay Dating App and Visited LGBT Nightclub on Other Occasions, Witnesses Say," *Los Angeles Times*, June 13, 2016.

Hernandez, Joe, and Jaclyn Diaz, "The Police Response at Robb Elementary Was a Failure, a Texas Official Says," NPR, June 21, 2022.

Hesterman, Jennifer, *Soft Target Hardening: Protecting People from Attack*, Routledge, 2018.

Hillard Heintze, *The City of Virginia Beach: An Independent Review of the Tragic Events of May 31, 2019*, November 13, 2019.

Hollingsworth, Heather, "Unlocked Doors Were 'First Line of Defense' at Uvalde School," Associated Press, June 22, 2022.

Hollywood, John S., Richard H. Donohue, Tara Richardson, Andrew Lauland, Cliff Karchmer, Jordan R. Reimer, Thomas Edward Goode, Dulani Woods, Pauline Moore, Patricia A. Stapleton, Erik E. Mueller, Mark Pope, and Tom Scott, *Mass Attacks Defense Toolkit*, RAND Corporation, TL-A1613-1, 2022. As of October 6, 2023:
https://www.rand.org/pubs/tools/TLA1613-1.html

Hollywood, John S., Richard H. Donohue, Tara Richardson, Andrew Lauland, Cliff Karchmer, Jordan R. Reimer, Thomas Edward Goode, Dulani Woods, Pauline Moore, Patricia A. Stapleton, Erik E. Mueller, Mark Pope, and Tom Scott, "About the Mass Attacks Defense Toolkit," RAND Corporation, webpage, 2022. As of October 6, 2023:
https://www.rand.org/pubs/tools/TLA1613-1/toolkit/about.html

Holpuch, Amanda, and Emma Bubola, "23 Shot, 1 Fatally, at a Juneteenth Celebration in Illinois," *New York Times*, June 18, 2023.

Houses of Worship Committee, Cultural Properties Council, ASIS International, "Recommended Best Practices for Securing Houses of Worship Around the World," undated.

Huddy, Jon, "Design Considerations for a Safer Emergency Department," American College of Emergency Physicians, 2017.

Huskey, Michael G., and Nadine M. Connell, "Preparation or Provocation? Student Perceptions of Active Shooter Drills," *Criminal Justice Policy Review*, Vol. 32, No. 1, February 2021.

IES—*See* Institute of Education Sciences.

Institute of Education Sciences, U.S. Department of Education, "School Pulse Panel," webpage, undated. As of May 18, 2023:
https://ies.ed.gov/schoolsurvey/spp/

Interagency Security Committee, *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*, December 2015.

Investigative Committee on the Robb Elementary Shooting, Texas House of Representatives, *Interim Report 2022: A Report to the House of Representatives, 88th Texas Legislature,* July 17, 2022.

Irwin, Véronique, Ke Wang, Jiashan Cui, and Alexandra Thompson, *Report on Indicators of School Crime and Safety: 2021*, National Center for Education Statistics, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, NCES 2022-092/NCJ 304625, June 2022.

Jackson, Brian A., Melissa Kay Diliberti, Pauline Moore, and Heather L. Schwartz, *Teachers' Views on School Safety: Consensus on Many Security Measures, but Stark Division About Arming Teachers*, RAND Corporation, RR-A2641-1, 2023. As of October 10, 2023:
https://www.rand.org/pubs/research_reports/RRA2641-1.html

Jackson, Brian A., Ashley L. Rhoades, Jordan R. Reimer, Natasha Lander, Katherine Costello, and Sina Beaghley, *Practical Terrorism Prevention: Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence*, RAND Corporation, RR-2647-DHS, 2019. As of May 8, 2023:
https://www.rand.org/pubs/research_reports/RR2647.html

Johns Hopkins University Applied Physics Laboratory, *A Comprehensive Report on School Safety Technology*, version 2.0, U.S. Department of Justice, National Institute of Justice, October 2016.

Johnson, Sarah Lindstrom, Jessika Bottiani, Tracy E. Waasdorp, and Catherine P. Bradshaw, "Surveillance or Safekeeping? How School Security Officer and Camera Presence Influence Students' Perceptions of Safety, Equity, and Support," *Journal of Adolescent Health*, Vol. 63, No. 6, December 2018.

Jonson, Cheryl Lero, "Preventing School Shootings: The Effectiveness of Safety Measures," *Victims and Offenders*, Vol. 12, No. 6, 2017.

Jonson, Cheryl Lero, Melissa M. Moon, and Joseph A. Hendry, "One Size Does Not Fit All: Traditional Lockdown Versus Multioption Responses to School Shootings," *Journal of School Violence*, Vol. 19, No. 2, 2020.

King, Sanna, and Nicole L. Bracy, "School Security in the Post-Columbine Era: Trends, Consequences, and Future Directions," *Journal of Contemporary Criminal Justice*, Vol. 35, No. 3, August 2019.

Králová, Klaudia, Viktor Šoltés, and Nikol Kotalová, "Protection of Transport Terminals Through the Application of the CPTED Concept," *Transportation Research Procedia*, Vol. 55, 2021.

Lankford, Adam, and Eric Madfis, "Media Coverage of Mass Killers: Content, Consequences, and Solutions," *American Behavioral Scientist*, Vol. 62, No. 2, February 2018.

Lankford, Adam, and James Silver, "Why Have Public Mass Shootings Become More Deadly? Assessing How Perpetrators' Motives and Methods Have Changed over Time," *Criminology and Public Policy*, Vol. 19, No. 1, February 2020.

Las Vegas Metropolitan Police Department, *1 October After-Action Review*, circa June 2019.

Lee, Jae Yong, Kayla Ostrowski, and J. Eric Dietz, "Effectiveness of Unarmed Response to Active Shooter Incidents," poster for 24th annual security symposium, Center for Education and Research in Information Assurance and Security, March 28–29, 2023.

Lemoine, Bret, "Waukesha Memorial Day Parade Returns; Traffic Barricades in Place," FOX6 Milwaukee, May 30, 2022.

Leonard, Herman B. "Dutch," Christine M. Cole, Arnold M. Howitt, and Philip B. Heymann, Why *Was Boston Strong? Lessons from the Boston Marathon Bombing*, Harvard Kennedy School Program on Crisis Leadership, April 2014.

Los Angeles Police Department, *An Examination of May Day 2007*, report to the Board of Police Commissioners, October 9, 2007.

Manchester Arena Inquiry, *Report of the Public Inquiry into the Attack on Manchester Arena on 22nd May, 2017*, Vol. 1: *Security for the Arena*, HC 279, June 2021.

Marjory Stoneman Douglas High School Public Safety Commission, *Initial Report Submitted to the Governor, Speaker of the House of Representatives and Senate President*, January 2, 2019.

Mascall, Kandis, and Bill Hutchinson, "Nashville School Shooting Puts Renewed Focus on Doors, Security," ABC News, March 28, 2023.

Massachusetts Emergency Management Agency, Massachusetts Department of Public Health, City of Boston, City of Cambridge, Town of Watertown, Massachusetts Bay Transportation Authority Transit Police Department, Massachusetts National Guard, and Massachusetts State Police, *After Action Report for the Response to the 2013 Boston Marathon Bombings*, December 2014.

McCauley, Kristin, *Investigative Report: Arapahoe High School Case CT13-44545*, Office of the Sheriff, Arapahoe County, Colorado, undated.

Metropolitan Police Department Internal Review Team, *After Action Report: Washington Navy Yard, September 16, 2013: Internal Review of the Metropolitan Police Department, Washington, D.C.*, July 2014.

Miami-Dade County Public Schools, "It's No Joke," webpage, undated. As of June 25, 2023: https://itsnojoke.dadeschools.net/#!/rightColumn/2641

Ministry of Foreign Affairs of the People's Republic of China, "Gun Violence in the United States: Truth and Facts," February 16, 2023.

Moore, Pauline, Brian A. Jackson, Catherine H. Augustine, Elizabeth D. Steiner, and Andrea Phillips, *A Systems Approach to Physical Security in K–12 Schools*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-A1077-1, 2021. As of March 10, 2022:
https://www.rand.org/pubs/research_reports/RRA1077-1.html

Moore-Petinak, N'dea, Marika Waselewski, Blaire Alma Patterson, and Tammy Chang, "Active Shooter Drills in the United States: A National Study of Youth Experiences and Perceptions," *Journal of Adolescent Health*, Vol. 67, No. 4, October 2020.

Mosbergen, Dominique, "Walmart Employee Helped More Than 100 People Escape El Paso Shooting," *Huffington Post*, August 7, 2019.

MSDHS Public Safety Commission—*See* Marjory Stoneman Douglas High School Public Safety Commission.

Na, Chongmin, and Denise C. Gottfredson, "Police Officers in Schools: Effects on School Crime and the Processing of Offending Behaviors," *Justice Quarterly*, Vol. 30, No. 4, 2013.

Nance, Jason P., "Student Surveillance, Racial Inequalities, and Implicit Racial Bias," *Emory Law Journal*, Vol. 66, No. 4, 2017.

National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; National Cooperative Highway Research Program; Countermeasures Assessment and Security Experts; and Western Management and Consulting, *Update of Security 101: A Physical Security and Cybersecurity Primer for Transportation Agencies*, National Academies Press, 2020.

National Academies of Sciences, Engineering, and Medicine; Transportation Research Board; Transit Cooperative Research Program; and Ernest "Ron" Frazier, *Policing and Security Practices for Small- and Medium-Sized Public Transit Systems*, National Academies Press, 2015.

National Association of School Psychologists, National Association of School Resource Officers, and Safe and Sound Schools, *Best Practice Considerations for Armed Assailant Drills in Schools*, December 2014, updated April 2021.

National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education, "Fast Facts: School Safety and Security Measures," webpage, undated. As of May 18, 2023:
https://nces.ed.gov/fastfacts/display.asp?id=334

National Center for Education Statistics, Institute of Education Science, U.S. Department of Education, *Safety and Security Practices at Public Schools*, last updated May 2022.

National Center for Spectator Sports Safety and Security, University of Southern Mississippi, *Interscholastic Athletics and After-School Safety and Security: Best Practices Guide*, 6th ed., last updated July 2020.

National Center on Safe Supportive Learning Environments, U.S. Department of Education, "School Climate Improvement," webpage, undated. As of July 25, 2023:
https://safesupportivelearning.ed.gov/school-climate-improvement

National Crime Prevention Council, "Sell with Certainty," webpage, undated. As of June 19, 2023:
https://www.sellwithcertainty.org/

National Police Foundation, *After-Action Review of the Orlando Fire Department Response to the Attack at Pulse Nightclub*, October 2018.

National Police Foundation, *Preparing for and Responding to Mass Demonstrations and Counter-Demonstrations in Portland, Oregon: A Review of the Portland Police Bureau's Response to Demonstrations on June 14, 2017, August 4, 2018, and August 17, 2019*, December 2020.

National Shooting Sports Foundation, "5 Ways the Firearm Industry Is Helping to Keep Guns Out of the Wrong Hands," January 1, 2021.

National Threat Assessment Center, U.S. Secret Service, U.S. Department of Homeland Security, *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools*, March 2021.

National Threat Assessment Center, U.S. Secret Service, U.S. Department of Homeland Security, *Mass Attacks in Public Spaces: 2016–2020*, January 2023.

NCES—*See* National Center for Education Statistics.

NTAC—*See* National Threat Assessment Center.

Office of Community Oriented Policing Services, U.S. Department of Justice, "School Violence Prevention Program (SVPP)," webpage, undated. As of June 16, 2023:
https://cops.usdoj.gov/svpp

Owens, Emily G., "Testing the School-to-Prison Pipeline," *Journal of Policy Analysis and Management*, Vol. 36, No. 1, Winter 2017.

Peck, Robert A., "Security and Democracy: Designing Public Buildings for Safety and Accessibility," blog post, Gensler, January 15, 2021. As of May 18, 2023:
https://www.gensler.com/blog/security-and-democracy-designing-public-buildings-for-safety

Perumean-Chaney, Suzanne E., and Lindsay M. Sutton, “Students and Perceived School Safety: The Impact of School Security Measures,” *American Journal of Criminal Justice*, Vol. 38, No. 4, December 2013.

Peterson, Jillian, Violence Project, “The Violence Project,” presentation to the 2023 National Institute of Justice Conference, May 24, 2023.

Peterson, Jillian, Hamline University, and James Densley, Metropolitan State University, “Reflections on Researching the Lives and Crimes of Mass Shooters,” in National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, *Advancing Understanding, and Informing Prevention of Public Mass Shootings: Findings from NIJ Funded Studies*, Part 2, webinar slides, November 17, 2020.

Price, James H., and Jagdish Khubchandani, “School Firearm Violence Prevention Practices and Policies: Functional or Folly?” *Violence and Gender*, Vol. 6, No. 3, September 2019.

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002.

Reeping, Paul M., Sara Jacoby, Sonali Rajan, and Charles C. Branas, “Rapid Response to Mass Shootings: A Review and Recommendations,” *Criminology and Public Policy*, Vol. 19, No. 1, February 2020.

Reidman, David, “K–12 School Shooting Database,” webpage, undated. As of August 10, 2023:
https://k12ssdb.org/

Research and Special Programs Administration, John A. Volpe National Transportation Systems Center, *Transit Security Design Considerations: Final Report*, Office of Research Demonstration and Innovation and Office of Program Management, Federal Transit Administration, U.S. Department of Transportation, November 2004.

Rocque, Michael, “Exploring School Rampage Shootings: Research, Theory, and Policy,” *Social Science Journal*, Vol. 49, No. 3, September 2012.

RSMeans, homepage, undated. As of October 11, 2023:
https://www.rsmeans.com

Salman, Noor Zahi, motion to preclude improper argument in government’s opening statement, *United States v. Noor Zahi Salman*, U.S. District Court, Middle District of Florida, Orlando Division, case 6:17-cr-00018-PGB-KRS, document 287, filed March 5, 2018.

Schwartz, Heather L., Rajeev Ramchand, Dionne Barnes-Proby, Sean Grant, Brian A. Jackson, Kristin J. Leuschner, Mauri Matsuda, and Jessica Saunders, *The Role of Technology in Improving K–12 School Safety*, RAND Corporation, RR-1488-NIJ, 2016. As of October 11, 2023:
https://www.rand.org/pubs/research_reports/RR1488.html

Schwerin, Daniel L., Jeff Thurman, and Scott Goldstein, “Active Shooter Response,” *StatPearls*, StatPearls Publishing, last updated February 13, 2023.

Silva, Jason R., and Emily A. Greene-Colozzi, “What We Know About Foiled and Failed Mass School Shootings,” Regional Gun Violence Research Consortium, Rockefeller Institute of Government, State University of New York, August 2022.

Steiner, Elizabeth D., Andrea Phillips, Pauline Moore, Brian A. Jackson, and Catherine H. Augustine, *Challenges in Implementing Physical Security Measures in K–12 Schools*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-A1077-2, 2021. As of October 6, 2023:
https://www.rand.org/pubs/research_reports/RRA1077-2.html

Straub, Frank, Blake Norton, Jennifer Zeunik, Brett Meade, Ben Gorban, Rebecca Benson, Joyce Iwashita, Alyse Folino Ley, and Michael Johnson, *Recovering and Moving Forward: Lessons Learned and Recommendations Following the Shooting at Marjory Stoneman Douglas High School*, National Police Foundation and Center for Mass Violence Response Studies, August 2019.

Tanner-Smith, Emily E., Benjamin W. Fisher, Lynn A. Addington, and Joseph H. Gardella, "Adding Security, but Subtracting Safety? Exploring Schools' Use of Multiple Visible Security Measures," *American Journal of Criminal Justice*, Vol. 43, No. 1, March 2018.

TriData Division, System Planning Corporation, *Aurora Century 16 Theater Shooting: After Action Report for the City of Aurora, Colorado*, submitted to City of Aurora, April 2014.

U.S. Bureau of Economic Analysis, "Gross Domestic Product: Implicit Price Deflator (A191RI1Q225SBEA)," webpage, updated September 28, 2023. As of October 11, 2023:
https://fred.stlouisfed.org/series/A191RI1Q225SBEA

U.S. Bureau of Labor Statistics, "Producer Price Index by Commodity: All Commodities (PPIACO)," webpage, September 2023. As of October 11, 2023:
https://fred.stlouisfed.org/series/PPIACO

U.S. Census Bureau, "Investigation and Security Services, All Establishments, Employer Firms," January 2023.

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter III, Science and Technology in Support of Homeland Security; Section 185, Federally Funded Research and Development Centers.

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter XV, Homeland Security Grants; Section 601, Definitions.

U.S. Code, Title 46, Shipping; Subtitle VII, Security and Drug Enforcement; Chapter 701, Port Security; Subchapter I, General; Section 70103, Maritime Transportation Security Plans.

U.S. Department of Health and Human Services, grants.gov, homepage, undated. As of October 12, 2023:
https://www.grants.gov

U.S. Department of Homeland Security, "Mass Gatherings; Security Awareness for Soft Targets and Crowded Places," undated.

U.S. Department of Homeland Security, "Soft Target and Crowded Places Security Plan Overview," May 2018.

U.S. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019.

Violence Project, "Key Findings," webpage, undated. As of June 19, 2023:
https://www.theviolenceproject.org/key-findings/

Weber, Marcela C., Stefan E. Schulenberg, and Elicia C. Lair, "University Employees' Preparedness for Natural Hazards and Incidents of Mass Violence: An Application of the Extended Parallel Process Model," *International Journal of Disaster Risk Reduction*, Vol. 31, October 2018.

White, Elizabeth, "Four Killed, 28 Injured in Dadeville Shooting," WRBL News 3, April 16, 2023, updated April 17, 2023.

Williams, Alex, Emily Corner, and Helen Taylor, "Vehicular Ramming Attacks: Assessing the Effectiveness of Situational Crime Prevention Using Crime Script Analysis," *Terrorism and Political Violence*, Vol. 34, No. 8, 2022.

Zhu, Runhe, Gale M. Lucas, Burcin Becerik-Gerber, and Erroll G. Southers, "Building Preparedness in Response to Active Shooter Incidents: Results of Focus Group Interviews," *International Journal of Disaster Risk Reduction*, Vol. 48, September 2020.

Zycher, Benjamin, *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*, RAND Corporation, MR-1693-RC, 2003. As of March 8, 2023: https://www.rand.org/pubs/monograph_reports/MR1693.html

Attacks on soft targets and crowded places (ST-CPs) represent a significant challenge. The U.S. Department of Homeland Security requires research and development to assess methods for reducing the propensity and loss of life from these types of attacks. In response, researchers from the Homeland Security Operational Analysis Center conducted a comprehensive landscape assessment of the threat to ST-CPs and corresponding security measures. This assessment integrated literature reviews, attack plot analyses, grant data reviews, and security cost modeling to identify both needs for improvement and recommended research and investment priorities for addressing those needs.

The number of attack plots is broadly aligned with regional population counts. The most-common motivations for ST-CP attacks have been personal, followed by terrorist and extremist motivations. Education and private buildings (workplaces) are the most–frequently targeted types of ST-CPs. Attacks on ST-CPs that have large, accessible crowds, such as houses of worship, shopping malls, restaurants, bars, and nightclubs, had the highest average lethality.

To defend ST-CPs, a layered approach has security measures work together to improve the chance that an attack will be stopped or mitigated. Prevention measures stop attacks before they reach execution; however, the public needs to know what warning signs to look for and how to report them, and threat assessment teams need to assess tips and follow up appropriately. Access control systems, such as locks, secured windows, and secured entryways, have been effective and efficient. Bystanders and security have both stopped attacks; groups of bystanders tackling shooters have been highly effective.

$47.00

ISBN-10 197741261-0
ISBN-13 9781977412614

54700

9 781977 412614

Cover image credits: Gards/Getty Images (left),
Skynesher/Getty Images (top right),
Nikada/Getty Images (bottom right)

RR-A2260-1