HSOAC | HOMELAND SECURITY OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the RAND Corporation under contract with DHS

Research Report

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

Keeping Soft Targets and Crowded Places Safe from Mass-Casualty Attacks

Insights from a Landscape Assessment

In 2018, the U.S. Department of Homeland Security (DHS) released "Soft Target and Crowded Places Security Plan Overview" to provide key stakeholders in the public and private sectors with an overview of its mission to enhance security and resilience of soft targets (STs) and crowded places (CPs). The plan defines ST-CPs as including "sports venues, shopping venues, schools, and transportation systems . . . 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] Although they are relatively rare, ST-CP attacks result in significant loss of life: One type of attack—

KEY FINDINGS

- The most-common motivations for attacks are personal, followed by terrorism and extremism.
- Education and private buildings are the most–frequently targeted types of soft targets (STs) and crowded places (CPs).
- Attacks on ST-CPs with large, accessible crowds, such as houses of worship, shopping malls, restaurants, bars, and nightclubs, have the highest average lethality.
- Layered security strategies, in which measures work together, improve the chance that an attack will be prevented, halted, or mitigated.
- Tips from the public have prevented attacks. Public education on what to report and how, and support for threat assessment teams, would make tips more effective.
- Access control systems, such as locks, secured windows, and secured entryways, have been effective and efficient but need to be trained on and maintained.

(continued on next page)

KEY FINDINGS—CONTINUED

- Bystanders and security have both stopped attacks. Groups of bystanders tackling shooters have been highly effective. Training can make responses even more effective.
- Response command, control, and communications need to be improved. Alternatives to traditional, push-to-talk voice radio communications are needed.
- Security measures need more effectiveness and efficiency evaluations. The security community has growing interest in artificial intelligence (AI); evaluations of security systems with AI will be needed as those systems deploy.

active shootings—was responsible for 100 killed in 50 attacks in 2022 and for 103 killed in 61 attacks in 2021.[2] This contributes to an atmosphere of fear throughout American society. Improving ST-CP security is a major priority.

In response to these challenges, the DHS Science and Technology Directorate contracted the Homeland Security Operational Analysis Center (HSOAC), a federally funded research and development center operated by RAND, to carry out a landscape assessment of the ST-CP threat, major vulnerabilities of ST-CP sites, status of existing security measures and initiatives, and ways to improve the allocation of ST-CP security resources.[3] The full results of this study are documented in the report *Improving the Security of Soft Targets and Crowded Places: A Landscape Assessment*.[4] This report summarizes that larger report.

Abbreviations

AAR	after-action report
AI	artificial intelligence
CP	crowded place
DHS	U.S. Department of Homeland Security
HSOAC	Homeland Security Operational Analysis Center
K–12	kindergarten through grade 12
MADT	Mass Attacks Defense Toolkit
RDT&E	research, development, test, and evaluation
SME	subject-matter expert
ST	soft target

Methodology

This research project was intended to answer the following question: How can prevention, protection, and response and recovery investments reduce casualties from attacks on ST-CPs? To accomplish this, the analysis for this study consisted of a mixed-method methodology. The methodology included quantitative analyses of existing datasets, an extensive literature review of governmental and nongovernmental sources of protective-factor information, an analysis of incident after-action reports (AARs) and case studies of high-profile incidents, interviews with SMEs, and an analysis of security spending trends.

The information garnered from the different methods was combined to create a landscape assessment that identifies the key components in an attack chain and opportunities for future investments to stop attacks or lessen casualties. The assessment provides insights into where investments would most help in increasing security at ST-CP sites. From these insights, a research road map was created to guide future efforts in improving ST-CP security. This road map consists of recommendations for future investments in research, development, test, and evaluation (RDT&E) and other funding and policy priorities.

Data Sources

The Mass Attacks Defense Toolkit

The primary data used for the quantitative analysis were those collected for the previously conducted Mass Attacks Defense Toolkit (MADT) project. The MADT drew on 27 existing datasets to identify 628 mass-attack plots, including foiled plots, failed plots, and completed attacks, from 1995 through 2020. The dataset consisted of every 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, but it excluded noncriminal and domestic-violence incidents in which the public was not involved and excluded terrorism cases prior to 2002, such as the September 11, 2001, terrorist attacks and Oklahoma City bombing. This project expanded the analysis of the MADT effort to include incident site configuration, incident site types, attributes associated with low-fatality incidents, and elements of attacker and bystander location during an incident, including elevation differences between attackers and bystanders, distances between attackers and bystanders, and movement of attackers or bystanders.[5]

The Literature Review and Case Study Analysis

An extensive literature review was conducted to capture past and existing federal, state, local government, and nongovernmental guidance, regulations, and recommendations related to protective factors for ST-CPs. We also searched the research literature, both peer-reviewed and non–peer-reviewed publications, and focused on the use of technology and physical security measures employed at ST-CP venues.

The literature review identified 178 sources published between 2002 and 2022 that contained information on protective measures employed at ST-CP venues. We also collected 22 AARs of mass attacks in public spaces authored by law enforcement organizations, federal agencies, law enforcement research institutes, and independent commissions.

In addition to the literature review, we conducted six case studies of high-profile ST-CP attacks between 2013 and 2021. The purpose of the case studies was to compare key aspects of the incidents and evaluate factors that might have affected the number of fatalities.[6]

Interviews

We conducted semistructured SME interviews to gain insights into the existing state of the ST-CP security environments, security practices, emerging technologies, and cost trends. We chose the interview candidates from a diverse group of security specialists. These included regional law enforcement personnel and intelligence specialists, security industry system integrators, cost experts, technology vendors, and security industry association leaders.

Cost-Model Inputs

The cost model used different data sources to determine the effort's scope (i.e., what security strategies to include), the unit cost of the security hardening strategies, and the appropriate quantity. We reviewed academic and industry literature to determine the appropriate measures to implement within a school to protect against potential mass attacks. The next step was assigning unit costs for each of the security and safety hardening measures. We relied primarily on the construction cost–estimating software RSMeans to estimate unit costs but also used industry literature. Last, we estimated the appropriate quantity through a parameterization based on the size of the school in square feet (e.g., the number of entrances per square foot) or the size of the school in enrollment (e.g., number of security guards per student).

The Landscape Assessment

We combined the information gathered in the quantitative analysis, literature review, interviews, and spending analysis to create a landscape assessment. The findings drove recommendations for funding and policy changes, as well as RDT&E efforts. Using those findings, we generated an innovation road map to improve ST-CP defenses; Figure 1 illustrates this process.

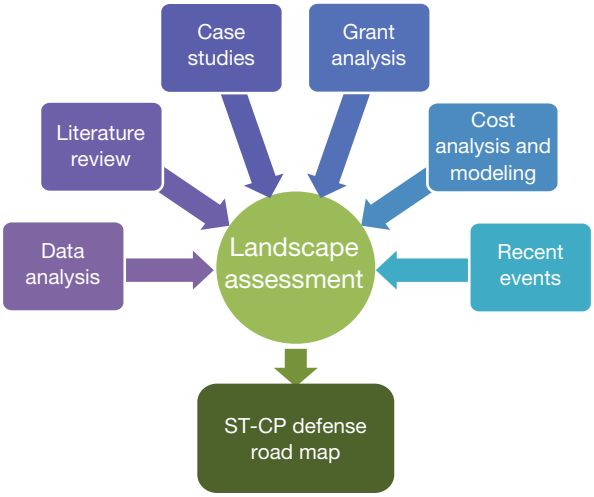
The Nature of the Threat and Protective Measures

A Summary of the Threat to Soft Targets and Crowded Places

The ST-CP threat landscape has changed in the past 30 years. This includes an evolution in the type of threat actor, the rise in the number of mass shootings, and the nature of the online environment that allows perpetrators to broadcast their actions. Research also shows that the ST-CP threat is primarily from mass shootings, although knife, explosive, and vehicle-ramming attacks are part of the overall threat environment.

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-inspired motivations) to more-individual attacks by a perpetrator with personal grievances against specific groups or those with "poly-grievances or unknown motivations."[7] By far, the most plots have been for personal reasons (both formally stated and unstated, 63 percent), followed by ideological motivations, such as al Qaeda– and Daesh-related plots (19 percent), then domestic extremist motivations (17 percent).

FIGURE 1
Landscape-Assessment Structure



Plots for some of the ideological motivations—notably, for al Qaeda and Daesh and for militia-related violent extremism—were significantly likelier to be foiled in advance than attacks conducted for personal grievances. This could be because of the high-profile nature of the threat actor and the attention that the U.S. government and law enforcement give them. Ideological plots also tended to be more complicated and involve more people, thus leading to a greater chance of discovery. In contrast, a perpetrator planning an attack for personal reasons might well not speak with anyone about their motivations and intentions, increasing the likelihood of proceeding undetected.

The online environment has also changed the nature and impact of ST-CP attacks. Online chatrooms, blogs, and the ability to live stream events have given potential attackers the ability to connect with audiences globally in an effort to seek fame or spread their message. These types of online forums provide the ability for attackers to connect with like-minded people and post manifestos explaining their actions.

The data showed little concentration by geographic region. In terms of threat to specific types of venues, the most plots by far were against educational facilities (schools, colleges, and universities). Other locations with comparatively high numbers of plots included private buildings (workplaces), government facilities, houses of worship, open streets, and restaurants, bars, and nightclubs.

Fatalities caused by attacks at these types of venues were the highest for outdoor events, although the average was skewed because of the high number of fatalities suffered during the Route 91 Harvest Festival attack in Las Vegas in 2017. Other types of locations with high average numbers of fatalities include houses of worship, shopping malls, buildings on military facilities, and restaurants, bars, and nightclubs.

By far, the most plots have been for personal reasons, followed by ideological motivations, such as al Qaeda– and Daesh-related plots, then domestic extremist motivations.

The denseness of a crowd present at a venue and the type of weapon the attacker chose increased the likelihood of a high-fatality event. Handguns were most often used in attacks, causing more attack fatalities than any other weapon type. The second-most fatalities were caused by attacks using multiple guns, and the third-most fatalities were caused by rifle attacks.

A Summary of Protective Measures

The most-common types of protective measures identified in the literature review and case studies were

- closed-circuit television
- physical barriers
- entry screening and access points
- law enforcement or security personnel presence
- detection technology
- environmental and interior design.

Although a great deal of information exists on what measures are being employed and their expected benefit, evidence about the effectiveness of protective measures to prevent, mitigate the outcome of, and respond to attacks against soft targets is largely inconclusive and heavily context dependent. What little evidence does exist is based primarily on anecdotes or descriptive analysis and often yields mixed results. Another complication is that contextual factors affect the effectiveness of measures. As noted above, certain factors, such as the behavior of building occupants during emergencies, occupants' awareness of how various countermeasures work, and the nature of incidents themselves (insider versus outside attacks), can affect whether a security technology will have its intended benefit.

Although the efficacy of protective measures is not well understood, the research identified several important points about the implementation of protective measures at a venue. First, a critical component in protection is gaining information on an attack before it has commenced so it can be stopped. Our research indicated that preattack information came from four sources: tips from the public; individuals' associations with terrorist or extremist organizations; suspicious activity, such as online postings; and discoveries made from law enforcement investigations. Information from the MADT dataset indicated that attacks were thwarted 80 percent of the time when initial clues were reported or acted upon and that tips from the public were responsible for almost two-thirds of initial clues.

For facility security measures, the research pointed to access control systems—notably, locks that were properly installed, maintained, and used—as being effective and comparatively inexpensive. The research also pointed to having dedicated security managers as being effective and efficient.

In terms of reducing casualties, the research points to several courses of action. Direct action by bystanders can stop or shorten an attack when it occurs. Overall, the data make clear that, if confronted directly with a shooter, bystanders should immediately attempt to tackle and disarm the shooter. This was the most frequent and consistently effective intervention. Group tackling successfully stopped shootings in the dozen times it happened, and individuals were always at least partly successful and were fully successful in four of five attempts. Armed responses by guards, on-scene officers (typi-

cally off-duty), and, occasionally, civilian bystanders were often effective at stopping shooters. However, they were sometimes ineffective in cases in which an armed responder could not or failed to engage (could not reach the shooter for whatever reason) or the shooter shot the armed responder first.

Once an attack begins, coordination of response assets is critical and requires joint training to be effective. Training and response drills improve readiness and response and can lead to fewer and less severe casualties. These drills are most effective when they expand participation beyond the standard group of law enforcement, venue security, and medical response personnel to also include facility employees, volunteers, patrons, and members of the public. Cross-agency coordination and training are critical for responding agencies to understand who is in command on scene and what information is available and to deconflict communications.

However, there could be unintended consequences of employing some measures in certain locations. Several security experts with whom we spoke stated that many venue operators wanted to create a welcoming atmosphere at their venues, whether it is a sports arena, house of worship, or a school. The addition of overt security apparatus, such as cameras and metal detectors, can create a more threatening environment for a venue's patrons. Additionally, measures that restrict the flow of people into a venue can create long lines or large crowds outside the secured areas, thus creating an attractive target for a would-be attacker who would not even have to gain access to the venue to conduct a mass-casualty attack.

Another emerging consideration is the growth of artificial intelligence (AI) technology. Although the term *AI* has different meanings depending on an individual's personal perceptions and AI itself is still a technology in its infancy, many security experts point to it as a future capability in protecting ST-CP sites. Some existing video analytic technologies can alert security personnel to someone who is behaving suspiciously or might have a weapon hidden in their clothing. Likewise, virtual fencing can alert security when an unauthorized person penetrates a venue's perimeter and expedite response.

The Potential of Cost Modeling for Improving Venue Security

An Overview of Grant Programs

For this research project, we conducted an extensive search of available federally sponsored security grants to better understand the resources available to state, local, tribal, and territorial jurisdictions and other organizations to increase ST-CP security. These grants, originating from several federal agencies, include DHS's Homeland Security Grant Program and Urban Area Security Initiative, the U.S. Department of Transportation's Capital Investment Grants program and Airport Improvement Program, and the U.S. Department of Justice's Students, Teachers, and Officers Preventing (STOP) School Violence Act Program. These funds, measuring in the billions of dollars per year, are meant to assist with hardening ST-CP venues and the public to terrorism, mass vio-

Measures that restrict the flow of people into a venue can create long lines or large crowds outside the secured areas, thus creating an attractive target for a would-be attacker who would not even have to gain access to the venue to conduct a mass-casualty attack.

lence, and other threats. We performed this search to understand how grant funding was spent on ST-CP security, which protective and response measures were funded, and how specific venues used grant funding for their operating environments.

Ample information was available on the details of these grant programs, including qualifying applicants, administration of funds, and criteria for successful applications. What was lacking, however, was how these funds were actually spent after they had been awarded. We could not locate any publicly available information that provided specific details about how applicants spent their funding. Therefore, it was difficult to draw any conclusions on the efficacy of the programs other than to say that federal resources were available for governments and venue operators for ST-CP security.

An Overview of Cost Modeling

The amount of spending on school security products and services in the United States is considerable. In 2017 and 2021, schools and colleges in the United States invested approximately $2.7 billion and $3.1 billion, respectively, on improving security in facilities through such strategies as installing high-resolution security cameras with facial recognition software, training staff and students on security protocols, and making improvements to doors and locks.[8] However, the implementation of school security strategies has not been consistent across all schools throughout the United States. As of 2020, for instance, approximately 9 percent of public schools did not have security cameras to monitor school activity, and approximately 23 percent of public schools did not require faculty and staff to wear badges or picture identification.[9] To better understand the nature and order of magnitude of spending on school security at a national level, we developed a bottom-up cost model to estimate costs for implementing safety and security hardening strategies for kindergarten through grade 12 (K–12) public schools.

The safety and security strategies included in the cost model are based on (1) a system approach to physical security for K–12 schools developed by a team of HSOAC researchers and (2) standards and guidelines produced by ASIS International.[10] Table 1 lists the items included in the cost modeling.

For each item in the cost model, we assigned a unit cost and quantity. Given unit cost uncertainties, the cost model includes a range of unit costs for each item based on a minimum, mean, and maximum.[11] Similarly, we accounted for uncertainties in school sizes (as measured through student population or gross square footage of the school facilities) using the following distribution points: minimum, 25th percentile, mean, median, 75th percentile, 95th percentile, and maximum.

After establishing a unit cost and quantity for each safety and security measure, we calculated the extended cost of each item and arrived at a total cost per school. From there, we scaled up the total annualized cost per school by multiplying the costs by the

TABLE 1
Cost Categories Included in 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 public address 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
	School resource officers and programs

total number of public schools in the United States. Finally, we added factors to account for safety and security strategies already in use (and hence paid for). For instance, we applied a 91-percent reduction to the costs in the surveillance technology category because approximately 91 percent of public schools in the United States had already installed security cameras.

According to the model, the total annualized costs in 2022 dollars at a per-school level, per–school district level, and national level are estimated at approximately $251,600, $3.2 million, and $20.5 billion, respectively.[12] The model accounts for a range of costs based on different assumptions of unit costs (minimum, mean, and maximum) and quantities (minimum, 25th percentile, mean, median, 75th percentile, 95th percentile, and maximum) for a total of 21 possible combinations. Several factors contribute to the variation in these assumptions, 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). Table 2 summarizes the annualized costs for three scenarios of unit cost and quantity, and Table 3 presents a similar overview of annualized costs but for only the nonlabor elements of school safety and security hardening measures.

Labor constitutes a significant portion of the total estimated costs for safety and security hardening strategies. For instance, approximately 45 percent of the total costs are attributed to labor for security guards and approximately 37 percent of the total costs are attributed to resources for school safety and security programs, such as training school staff. 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. A breakdown of the total estimated annualized costs per school is illustrated in Figure 2.

Assuming that the current allocation of funding for safety and security measures is valid, the cost model serves two primary functions.[13] First, the model can serve as a framework to help individual schools and school districts predict costs of enhancing safety and security measures. Although there is uncertainty in the model and it might not accurately calculate costs for budgetary purposes, individual schools can use the model as a guide to determine what safety and security measures to implement and the expected costs for each measure. The second primary function of the cost framework is supporting national-level decisionmaking about improving school safety and security hardening measures. National-level decisionmakers can use the model to estimate the scale of investment needed to implement school safety and security measures across the portfolio of public K–12 schools in the United States and compare those investments under different policies.

TABLE 2

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

TABLE 3

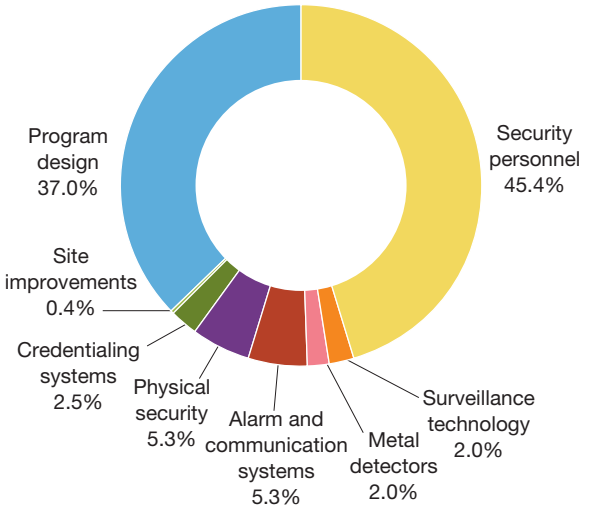
Total Cost for Nonlabor Elements of School Safety and Security Hardening Measures, in Millions of Dollars

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

FIGURE 2

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.

Although the cost model described here is specific to public K–12 schools, the framework can be applied to other facility types. For example, updated locks and doors, credentialing systems, and security guards can serve as protection measures in some venues, such as office buildings. For some other venues, however, the cost-estimating framework presented for schools might not be applicable and instead will require an alternative framework. For instance, estimating costs to implement safety and security strategies for a larger venue, such as a stadium or arena, is likely to benefit from a system- and operational-level approach in which event logistics, specific facility characteristics, and coordination with the existing security staff are considered.

A Landscape Assessment: Toward a Layered Model of Security for Soft Targets and Crowded Places

Forming the Model

The results from the quantitative data analysis, literature review, examination of AARs and case studies, interviews with SMEs, and cost analysis formed the landscape assessment of the current state of ST-CP threats, risks, and areas for improvement. HSOAC researchers have previously 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. In previous work, based on a K–12 setting, we have modeled defensive layers spatially, showing them on stylized site plans. Figure 3 illustrates this model.

From this earlier analysis, we developed a system-based conceptual model of the ST-CP attack chain and defensive layers, modifying the initial spatial representation to include the series of steps an attacker must complete in the attack chain to successfully carry out an attack. Figure 4 presents this model.

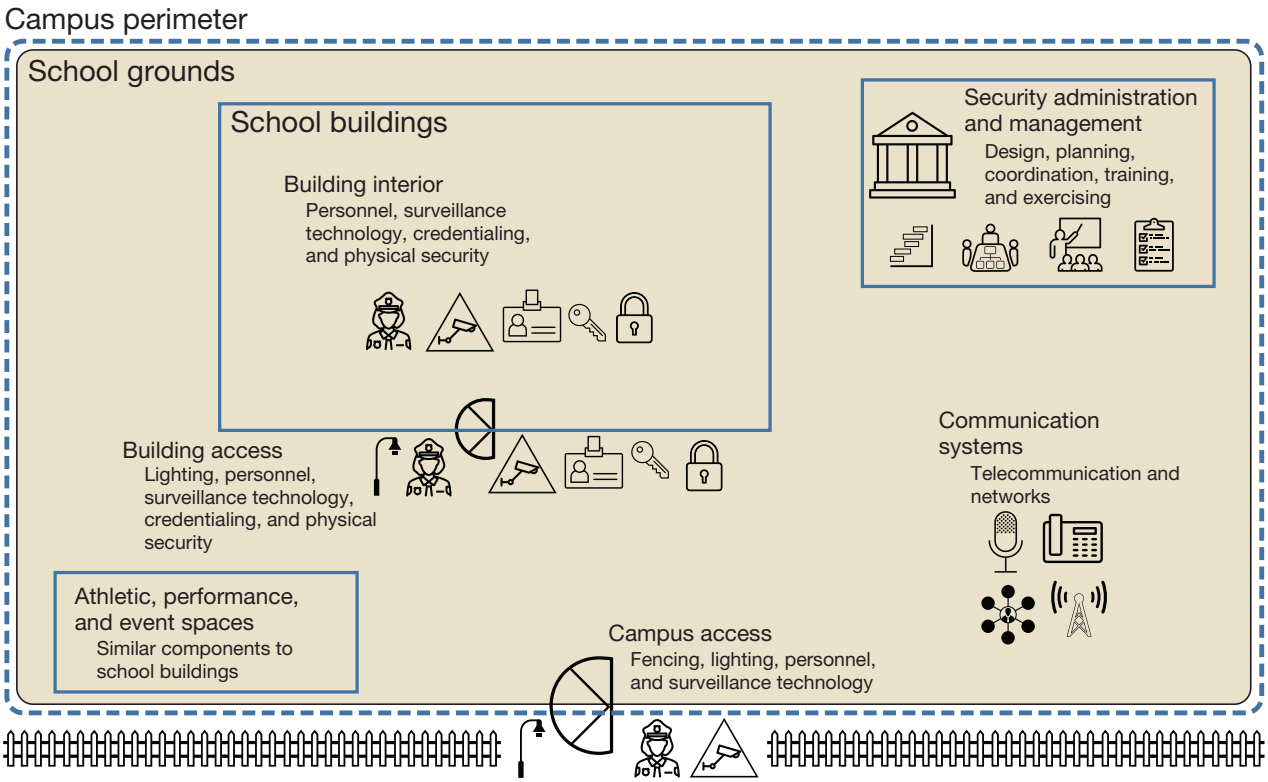
A system-based approach to physical security can help mitigate some of the challenges that ST facilities encounter when planning physical security improvements. These approaches situate physical security and protective measures as components of a broader approach to safety and security, including activities to prevent attacks 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 help facilities avoid single points of failure and both policies and training help reinforce and ensure the security benefits of protective measures.

Findings on Preventing Attacks

The first defensive layer of the ST-CP attack chain is prevention. A perpetrator must complete a series of steps to prepare for an attack, including becom-

FIGURE 3

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



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

ing motivated, planning, gathering materials, and conducting logistics activities. Each of these steps can present an opportunity for the plot to be discovered through observable activities, or leakage, such as social media posts or the purchase of weapons or ammunition. This leakage then provides opportunities for detection, often through tips from the public, to prevent the attack before it begins. Figure 5 illustrates the attack steps, corresponding measures to detect and stop attacks, and major findings and gaps about each.

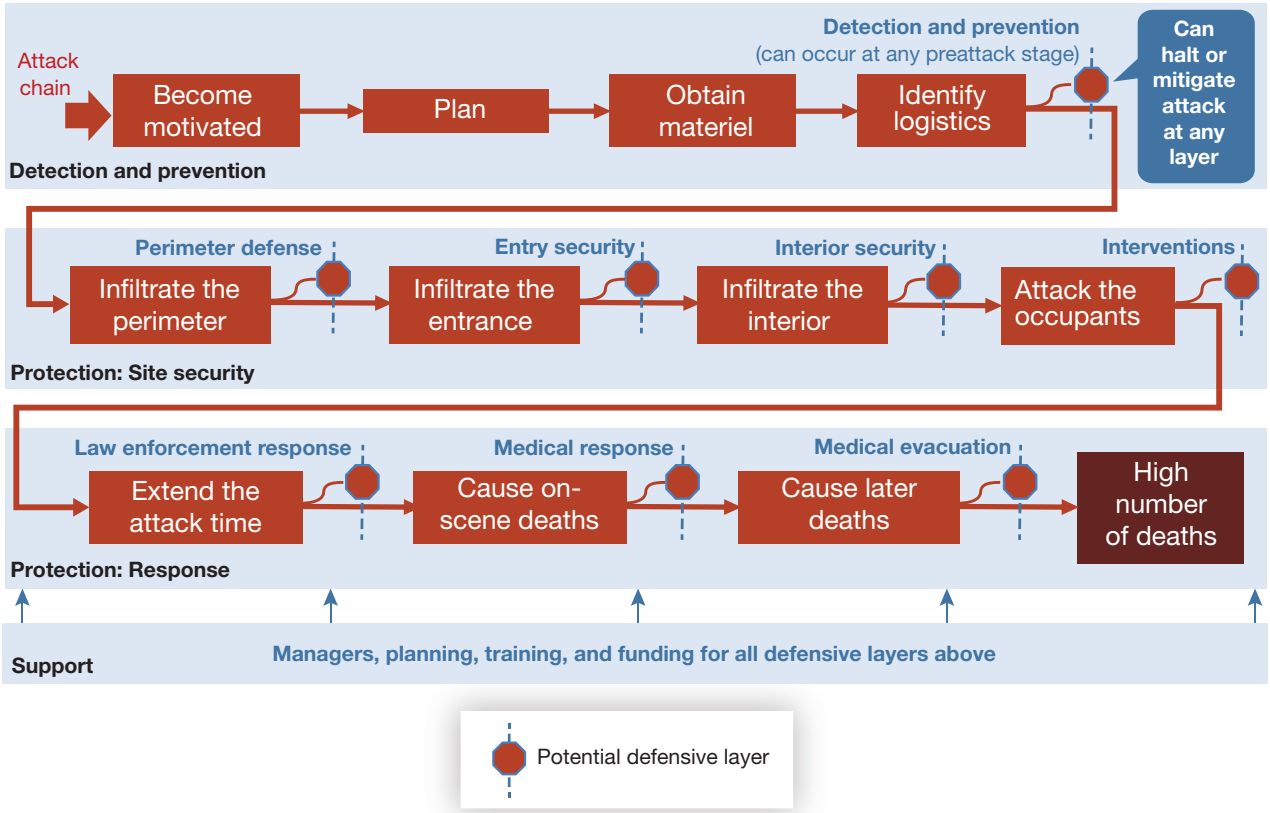
Guidance on what should be reported and on avenues for reporting is lacking. Tips from the public are the main source of initial clues in foiling an attack. Thus, there is a strong need to build on the ubiquitous "see something, say something" adage with more information on what to see (top indicators of potential plots) and how to say it (how to report it to authorities). In addition, information gathered online is not always easy for the public to report to authorities.

The number of false threats is high. Discussion at a 2023 National Institute of Justice conference included multiple comments that authorities in schools and elsewhere were being overwhelmed with false threats of mass shootings, taking up resources that could be much better spent on the few true threats.

Suspicious weapon- and ammunition-seeking behavior is not well understood. We found little material on the warning signs of someone attempting to acquire weapons and ammunition for attacks or on how to report them. There is a strong need to identify key indicators of gun and ammunition diversion while filtering out legitimate purchases (for, e.g., hunting, sporting) and development of subsequent education campaigns.

FIGURE 4

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



Site probing and breaching are not uncovered in time to prevent attacks. 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 discovered via on-scene surveillance and probing, implying an opportunity to find more plots by improving detection of these activities.

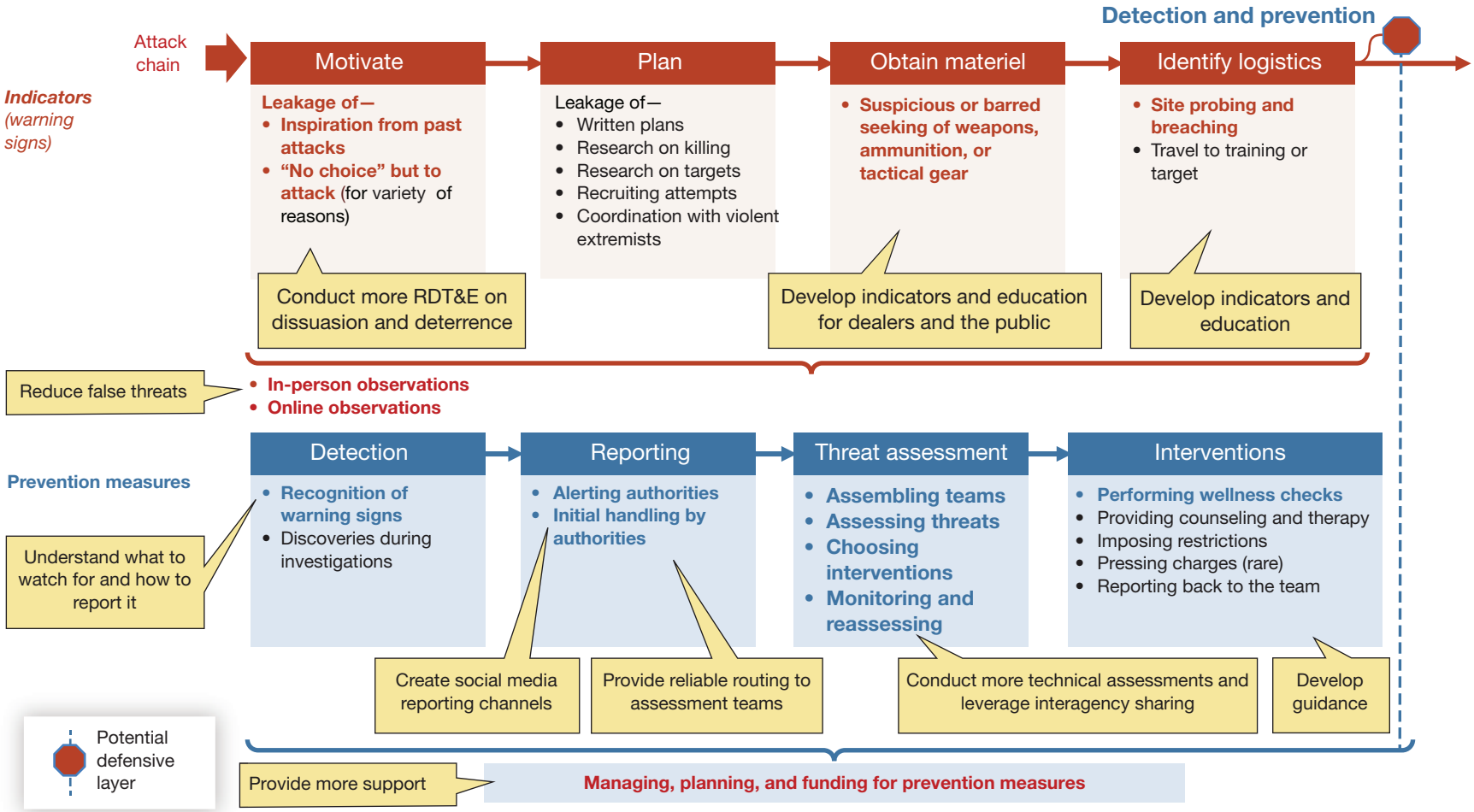
Findings on On-Site Security Measures

The second set of defensive layers in the ST-CP attack chain focuses on protective measures for on-site security. On-site security can be broken into three categories: open spaces, secured buildings, and major venues. *Open space* can be defined as an area that does not employ any access control measures. These can include parks and parking lots but also commercial establishments, such as malls, bars, and restaurants that allow direct access to patrons. Secured buildings, such as schools or office buildings, often utilize some kind of access control system to prevent unauthorized people from entering the facility. Major venues, such as arenas, theme parks, and airports, have security measures intended to screen people arriving on site for weapons and other contraband, in addition to controlled access and guards. These venues will likely have police and medical personnel on hand during events. Figure 6 illustrates on-site security defensive layers and key findings.

Security concepts for open and nonsecured spaces are not well developed. Little research exists for these types of spaces. The most-consistent security measure present is bystanders themselves. Therefore, measures are needed to provide the public with education and tools to report attackers more quickly or respond more effectively, either by leaving the scene earlier or by physically halting the attacker.

FIGURE 5

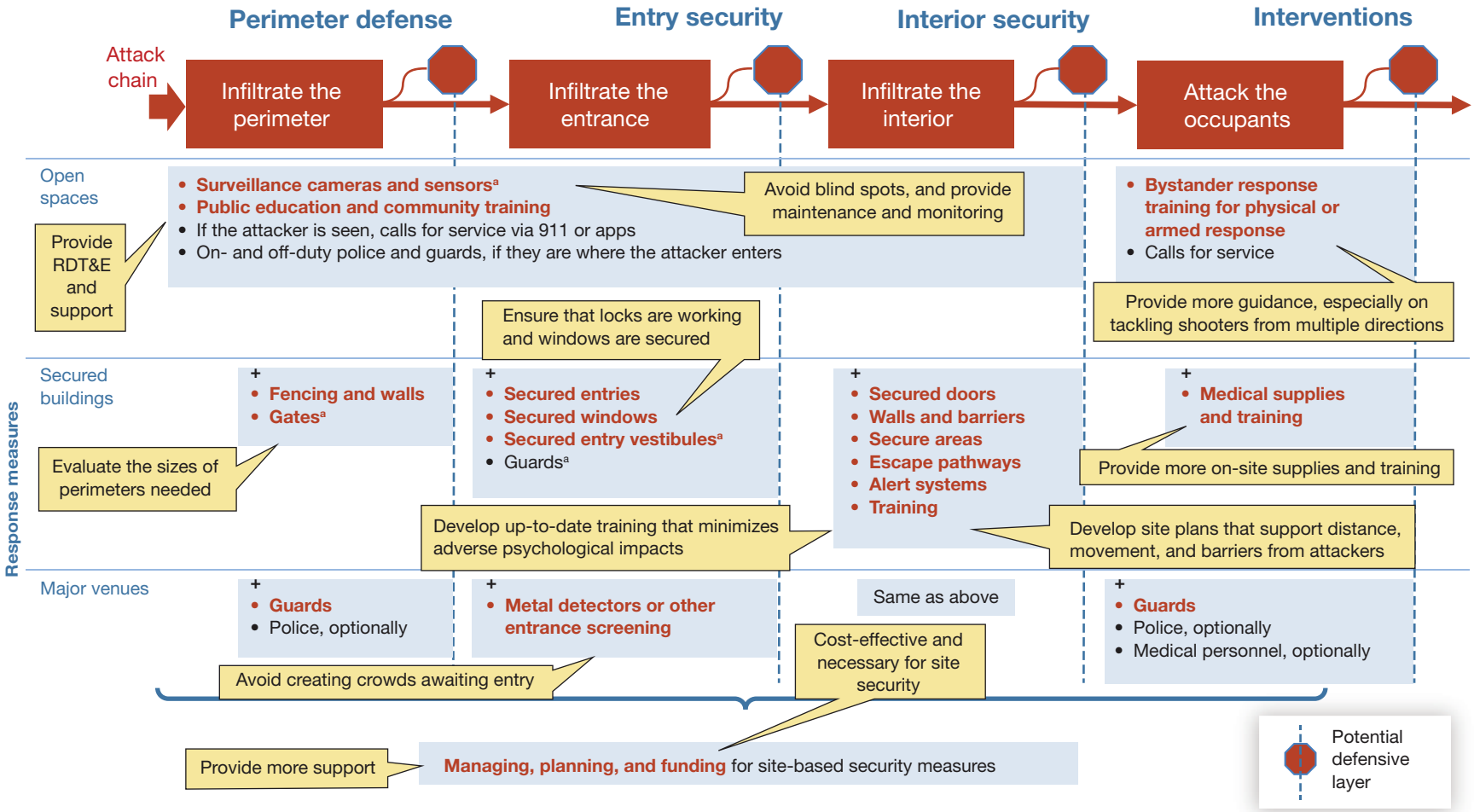
Prevention Layers of Security and Issues



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.

FIGURE 6

Protection: Site-Based Layers of Security and Issues



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.

Bystander response can be effective if bystanders know what works.

Additionally, there is a need to consider options and conditions for upgrading the security of open sites in a cost-effective, nonintrusive manner by possibly adding perimeter protections, additional entryways, layers of doors (external and internal), alarms, and capabilities to lock doors quickly.

Bystander response can be effective if bystanders know what works. This project largely validated the DHS "run, hide, and fight" concept of bystander response, although several clarifications are necessary. Most important is that the public needs more details about the fight concept. A bystander near a shooter, with less chance to successfully run or hide than a more distant bystander, is effectively in fight mode and must respond with overwhelming physical force. Instructions on the best techniques to subdue an attacker should be provided to the public. Additionally, armed responses have been effective but depend on a responder having the necessary training to stop an attack and being able to engage (e.g., not on the other side of a large complex from an attacker). When an armed responder is ineffective, unarmed security and bystanders should be ready to respond.

Some site plans could put more distance, movement, and barriers between would-be attackers and bystanders. Measures that disrupt an attacker's ability to surprise a crowd at close range are of high value. Secure outer perimeter defenses, such as fences, gates, and cameras, can ideally keep attackers far outside the site or at least provide the timeliest possible warning. Likewise, facilities with secure walkups and entry vestibules, in addition to locked doors and windows, provide an opportunity to keep an attacker from accessing the interior of a building. Secured pathways for bystanders to escape create time and distance from an attacker, as do sensors that provide early warning of a possible weapon-carrying attacker or a shooting as it occurs.

Secured doors and windows were the most-critical and -efficient measures but also had flaws in practice. Secured doors and windows can prevent attackers from entering a facility or limit their movement once inside; these measures can be highly effective and efficient. However, these measures failed in several mass shootings. Proper door and lock maintenance is necessary for the equipment to function properly. Although security film for windows does not make a window bulletproof, it does decrease an attacker's ability to easily enter through a window. Protocols for ensuring that doors and windows are locked are not always enforced.

Crowds awaiting entry to a venue become accessible targets. Security screening measures that create large external crowds waiting to go into a venue can create an accessible crowd for a would-be attacker.

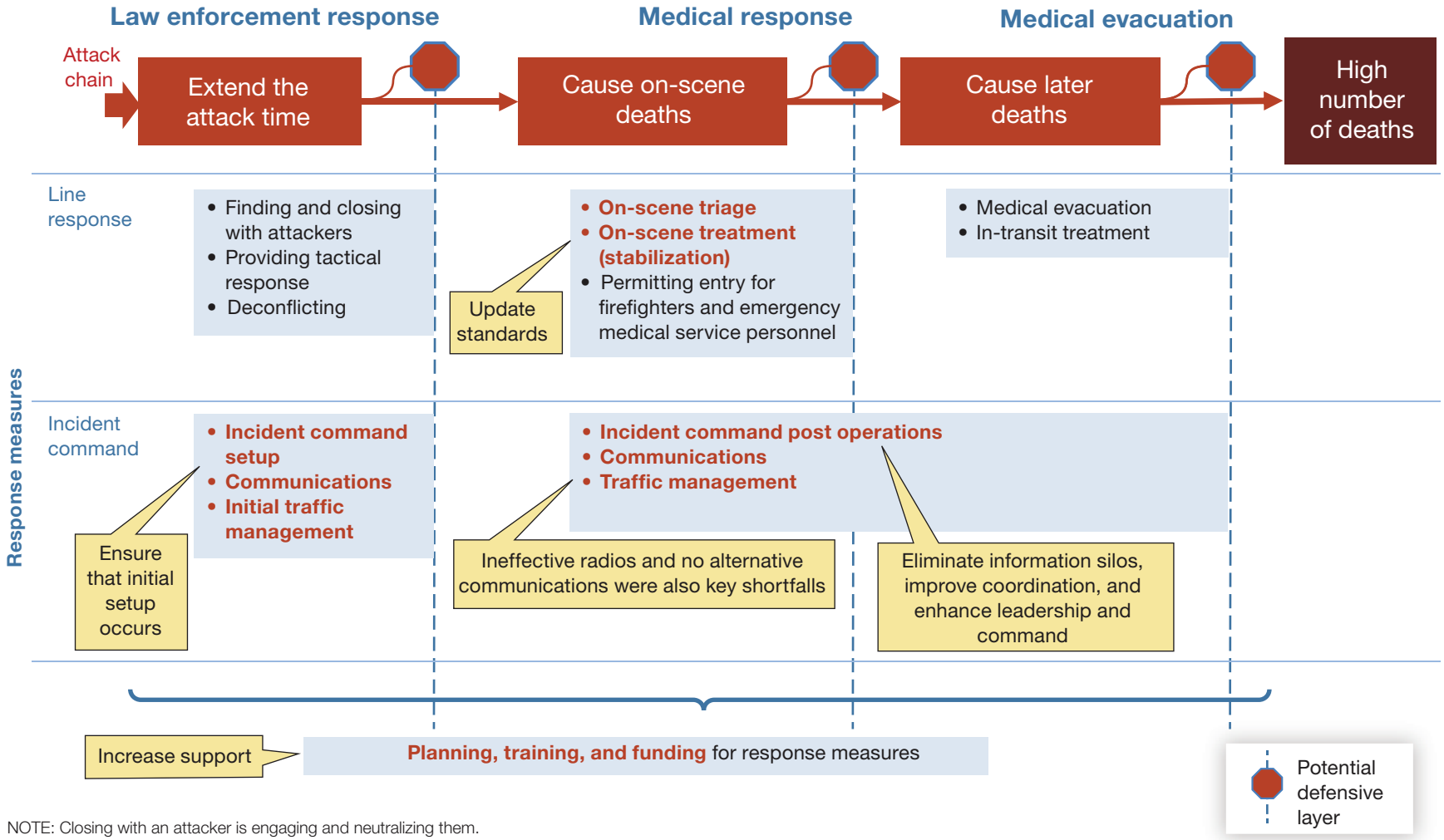
Findings on Responding to Attacks

The final layer in the security model addresses first responders' responses to attacks. This layer is intended to stop attacks as quickly as possible; minimize casualties during law enforcement's efforts to stop an attack; and maximize emergency medical personnel's ability to safely enter the venue, begin treatment, and evacuate casualties to definitive care. It also indicates the coordination and communication requirements to ensure that all responders can set up initial incident command protocols and successfully share information. Figure 7 illustrates the key aspects of this layer and key findings.

Incident command procedures and operations suffer from multiple issues. The literature review, AARs, and case studies indicated significant challenges with incident command operations, including initial setup, lack of clarity of roles, and dealing with an influx of responders. These cause delays in getting responders to the appropriate locations, addressing the threat, and providing medical assistance. To remedy these problems, AARs have suggested follow-

FIGURE 7

Protection: Response Layers of Security and Issues



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

Having a common framework, language for command, and agreements on roles and chains of command is critical to response.

ing National Incident Management System guidelines, having a common framework and language for command, having established agreements on roles and chains of command, and conducting joint training events. Providing responding agencies with plans and schematics of major ST-CP venues, such as schools, houses of worship, malls, theaters, and stadiums, in advance was also seen as a measure that could expedite awareness and command.

Communication is suboptimal both technically and operationally. Multiple AARs and case studies noted challenges with effective communication among first responders during an incident, such as radio interoperability, radio channel deconfliction where critical channels were getting overloaded and preventing situational awareness, and even lack of adequate radio-charging equipment. Proper procedures are needed to deconflict radio operations among the responding agencies and provide open channels so law enforcement and medical responders can provide assistance in a timely manner.

Multiagency coordination, planning, and training lack adequate support. Multiagency coordination, planning, and training can address issues related to incident response before attacks occur. Task assignment, communication, and incident command structure are all key components to successfully responding to and stopping an attack and providing medical assistance and evacuation. Having a common framework, language for command, and agreements on roles and chains of command is critical to response. These challenges can be addressed in multiagency training events.

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

Finally, this section presents the 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. In this report, we present only the most-important recommendations; the full report contains the complete list.

Research, Development, Test, and Evaluation Priorities

Improving Prevention

Seek Methods of 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. They 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 social validation of shootings that would-be attackers can experience online.[14]

Develop Indicators of and Education About Suspicious Seeking of Weapons

We recommend that developers 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;

Evaluation of security measures should include placement and monitoring for access controls, cameras, and shot sensors; the effectiveness of sensor and analysis systems intended to detect weapons or other kinds of attacks from greater standoff distances; and screening systems.

in some cases, someone has ready access to a firearm but not to hundreds or thousands of rounds of ammunition and corresponding magazines.

Develop Protocols and Education for Wellness Checks

We were unable to find formal guidance for conducting initial meetings with and assessments of those reported as being at high risk, despite the importance of such encounters. We recommend working with mental health and law enforcement personnel with experience in doing checks and following tips to develop these protocols.

Improving Protection

Further Evaluate the Effectiveness and Efficiency of Security Measures

We identified few studies examining the effectiveness or cost-effectiveness of security measures in stopping active shooters and other types of mass attacks. The comparative rarity of mass attacks hinders assessment of specific technologies based on past performance. Instead, we envision lab and exercise testing against simulated attackers. Alignment of products and nonmaterial measures with past attacks, plus performance with security proxies,[15] can also be analyzed.

According to our landscape-assessment results, topics should include placement and monitoring for access controls, cameras, and shot sensors; 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. We also anticipate evaluations of technologies incorporating AI features in coming years.

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 only constant elements are generally bystanders and their cell phones. Other security measures, including the presence of barriers, entry points, guards, and surveillance, are expected to be present intermittently. Concepts of operations for open and nonsecure spaces are needed that

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

Improving Defenses of Soft Targets and Crowded Places in General

Continuously Track and Analyze Mass-Attack Plots

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

Experts we interviewed emphasized that most threat assessments from tips end with some actions taken but no charges filed or publicized (commonly referred to as *the gray area*). The experts also mentioned that formal records about the numbers of such assessments are not available because of the sensitivities involved. We recommend considering survey research to estimate and characterize the annual numbers of threats that authorities regarded as credible but did not culminate in arrest because that will help agency planners, policymakers, and the public understand the true magnitude of activities conducted to prevent ST-CP attacks.

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 mass-shooting cases at ST-CP venues 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.

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

The sociopsychological impacts of mass attacks have been enormous and are further believed to have helped inspire would-be attackers. Potential reduction mechanisms might cover potential public health campaigns at both macro and micro levels, along with potential changes to immersive, saturation coverage of shootings.

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.
- **Ensure that funding and policy priorities reflect RDT&E findings** as they become available.

From a financial perspective, we have two recommendations. First, 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. We recommend that grant requirements and reporting systems be updated to track specific budgets and spending on ST-CP security items. Second, we recommend further development of cost-modeling tools to help security man-

The sociopsychological impacts of mass attacks, such as societal fear and secondary trauma, have been enormous and are further believed to have helped inspire would-be attackers.

Bystanders should be trained to tackle attackers the same way they would respond to aircraft hijackers post-9/11.

agers and other decisionmakers plan and budget for ST-CP security expenses.

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

This education and training should build on "see something, say something" principles and similar initiatives. This initiative 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 that sap attention from threat assessment teams. This effort can include supporting research to develop indicators (e.g., suspicious procurement of weapons or ammunition), better public education programs, and enhanced efforts to reduce the number of false threats.

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

To improve efficiency, this funding can cover threats besides mass attacks. Fusion centers can and should be leveraged to support these teams as needed. This effort can include supporting research to develop threat assessment analysis procedures that are more rigorous than existing assessment tools.

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

This education and training builds on run, hide, and fight principles. According to what we found, training should include the following:

- *Run* needs to include flight to areas secured away from attackers, not just outside.
- *Hide* needs to mean genuinely hidden—ideally, in an area locked away from a shooter. It should not include hiding under desks, under tables, or around walls or bookcases in ready view of a nonstationary shooter.
- *Fight* is mandatory if in close line of sight of 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, and attack from the back.") In general, bystanders should be trained to tackle shooters (or stabbers or other attackers) the same way they would respond to aircraft hijackers post-9/11.

Provide Additional Funding to Cross-Organizational Security Teams and Managers

Like with threat assessment teams, this 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 RDT&E for the open-space security concept of operations. 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

The 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 the site security updates described in the landscape-assessment floor plan discussion in particular.

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.

Fund Access Control Systems

This funding is especially needed for the basics of procurement and maintenance of locks, doors, windows, and security film for accessible glass windows and doors. The funding should also provide training on how to use the systems correctly.

Conclusion

Figure 8 summarizes the road map's recommendations, overlaid on the model of ST-CP attack steps and defensive layers. The figure shows recommendations to improve attack prevention, site security, and incident response, plus crosscutting recommendations.

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 in this road map, there are substantial opportunities to improve defenses further. By supporting key RDT&E and funding initiatives across the ST-CP defense chain and improving the system of layered defenses for ST-CP security in general, the country can reduce attacks and casualties.

FIGURE 8

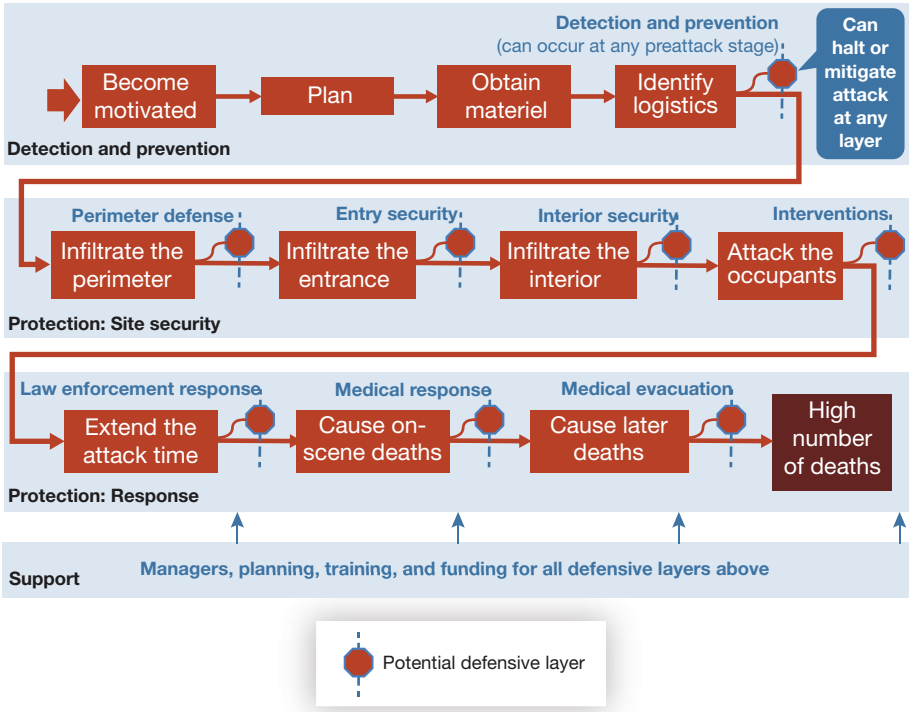
A Summary of the Road Map to Improve Security of Soft Targets and Crowded Places

Layered Security–General Priorities

General: help security measures work together to improve chance of halting the attack at any step

- More research, development, testing, and evaluation (RDT&E) on effectiveness of measures
- Security cost analyses
- Ongoing analysis of mass attacks, including high-casualty "crime" events
- Grant tracking
- Research and development on reducing mass psychological impacts of attacks

N.B.: High interest in AI



	Priority	
	Funding and Training	**Research and Development**
Detection and prevention	• What to report and how • Threat assessment teams	• Deterrence and dissuasion • Gun diversion indicators • Wellness-check protocols
Protection: Site security	• Security management teams • Bystander response • Access controls, starting with locks and windows • Medical supplies	• Concept of open-space security
Protection: Response	• Command, control, and communication	• Alternatives to traditional voice radio communication
Support	• Grant tracking • Attention to AI	• More RDT&E on the effectiveness of measures • Security cost analyses • Ongoing analysis of mass attacks, including high-casualty ordinary crimes • Reducing the mass psychological effects of attacks

Notes

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

[2] 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*, p. ii; 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*, p. 4.

[3] The landscape assessment incorporated information from data analysis, literature review, subject-matter expert (SME) interviews, and cost analysis to form a picture of the ST-CP security environment.

[4] Hollywood, Gierlack, et al., *Improving the Security of Soft Targets and Crowded Places*.

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

[6] The six cases studies were the 2013 Arapahoe High School shooting, the 2016 Pulse nightclub shooting, the 2017 Manchester Arena bombing, the 2018 Marjory Stoneman Douglas High School shooting, the 2019 El Paso Walmart shooting, and the 2021 Waukesha (Wisconsin) Christmas parade ramming.

[7] A polygrievance consists of multiple grievances that coalesce into a desire to act.

[8] Singer, "Schools Are Spending Billions on High-Tech Defense for Mass Shootings."

[9] National Center for Education Statistics, "Safety and Security Practices at Public Schools."

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

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

[12] These ranges of costs assume a mean unit cost and a mean unit of quantity.

[13] As stated in the literature review section, there is little research on the effectiveness of specific security measures. So this model, like the literature review, focuses only on where funding is being spent, not whether it is effective.

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

[15] 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.

References

ASIS International, *Physical Asset Protection*, Standard ASIS PAP-2021, 2021.

ASIS International, *Protection of Assets: Physical Security*, 2021 ed., 2021.

DHS—*See* U.S. Department of Homeland Security.

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.

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

Hollywood, John S., Keith Gierlack, Pauline Moore, Thomas Goode, Henry H. Willis, Devon Hill, Rahim Ali, Annie Brothers, Ryan Bauer, and Jonathan Tran, *Improving the Security of Soft Targets and Crowded Places: A Landscape Assessment*, Homeland Security Operational Analysis Center operated by the RAND Corporation, forthcoming.

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

National Center for Education Statistics, Institute of Education Science, U.S. Department of Education, "Safety and Security Practices at Public Schools," *Condition of Education 2022*, last updated May 2022.

Peterson, Jillian, and James Densley, "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.

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002.

Singer, Natasha, "Schools Are Spending Billions on High-Tech Defense for Mass Shootings," *New York Times*, June 26, 2022.

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. Department of Homeland Security, "Soft Target and Crowded Places Security Plan Overview," May 2018.

About the Authors

John Hollywood is a senior operations researcher at RAND, where he conducts decision science research in the areas of criminal justice, homeland security, and information technology. He has a Ph.D. in operations research.

Keith Gierlack is a senior defense analyst at RAND. His research addresses building partner capacity, law enforcement technology, critical infrastructure protection, maritime and border security, and China. He has an M.S. in strategic intelligence.

Pauline Moore is a political scientist at RAND. Her research focuses on violent extremism, targeted violence, terrorism and counterterrorism, and safety and security in K–12 schools. She holds a Ph.D. in international relations.

Tom Goode is a data scientist at RAND. His work focuses on national security, homeland security, and public safety. He has an M.S. in statistical practice.

Henry Willis is a senior policy researcher at RAND. His recent work has addressed biosecurity risks and biodefense capabilities; border and terrorism security; climate and natural disaster risks; critical infrastructure resilience; and national preparedness for chemical, biological, nuclear, and radiological attacks. He has a Ph.D. in engineering and public policy.

Devon Hill is a senior defense analyst at RAND. He has a particular interest in military personnel policy; defense acquisition; and talent management and diversity, equity, and inclusion. He has an M.A. in security studies.

Rahim Ali is a technical analyst at RAND. His research interests include critical infrastructure protection, community-level resilience planning, climate change adaptation and mitigation, and disaster preparedness and recovery. He has an M.S. in civil and environmental engineering.

Annie Brothers is an assistant policy researcher at RAND. Her research interests include workforce development, refugee resettlement, public safety, police–civilian communication, emergency response, behavioral health, domestic violence, and sexual assault. She has an M.S. in data science.

Ryan Bauer is a senior defense analyst at RAND. His research focuses on information warfare and information operations, disinformation and messaging, Russian security issues, and emergency preparedness. He has an M.A. in security studies.

Jon Tran is a senior technical analyst at RAND. He has supported and conducts research in the areas of policy related to national security, space, and aerospace systems. He has an M.S. in aerospace engineering.

About This Report

Attacks on soft targets (STs) and crowded places (CPs) represent a significant challenge in the 21st-century security environment. The U.S. Department of Homeland Security (DHS) requires research and development support to evaluate methods of reducing the propensity, 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, 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. This report describes and synthesizes work done to describe the ST-CP threat landscape and identify potential future research that could enhance ST-CP security. This is intended to be of interest to security and policy stakeholders at DHS and other federal, state, local, tribal, and territorial entities responsible for providing security and response services at the identified venues. This report should also be of interest to the public.

This research was sponsored by DHS's Science and Technology Directorate and conducted in the Infrastructure, Immigration, and Security Operations Program of the RAND Homeland Security Research Division (HSRD), which operates HSOAC.

This report presents the results of research and analysis conducted under task order 70RSAT22FR0000074, Soft Target and Crowded Places Landscape Assessment and Research Roadmap.

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the RAND Corporation under contract with DHS

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 the Homeland Security Operational Analysis Center (HSOAC) as an FFRDC for the U.S. Department of Homeland Security (DHS) 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 organized as a set of discrete tasks.

The information presented in this publication does 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, visit www.rand.org/t/RRA2260-2.

This research was published in 2024.