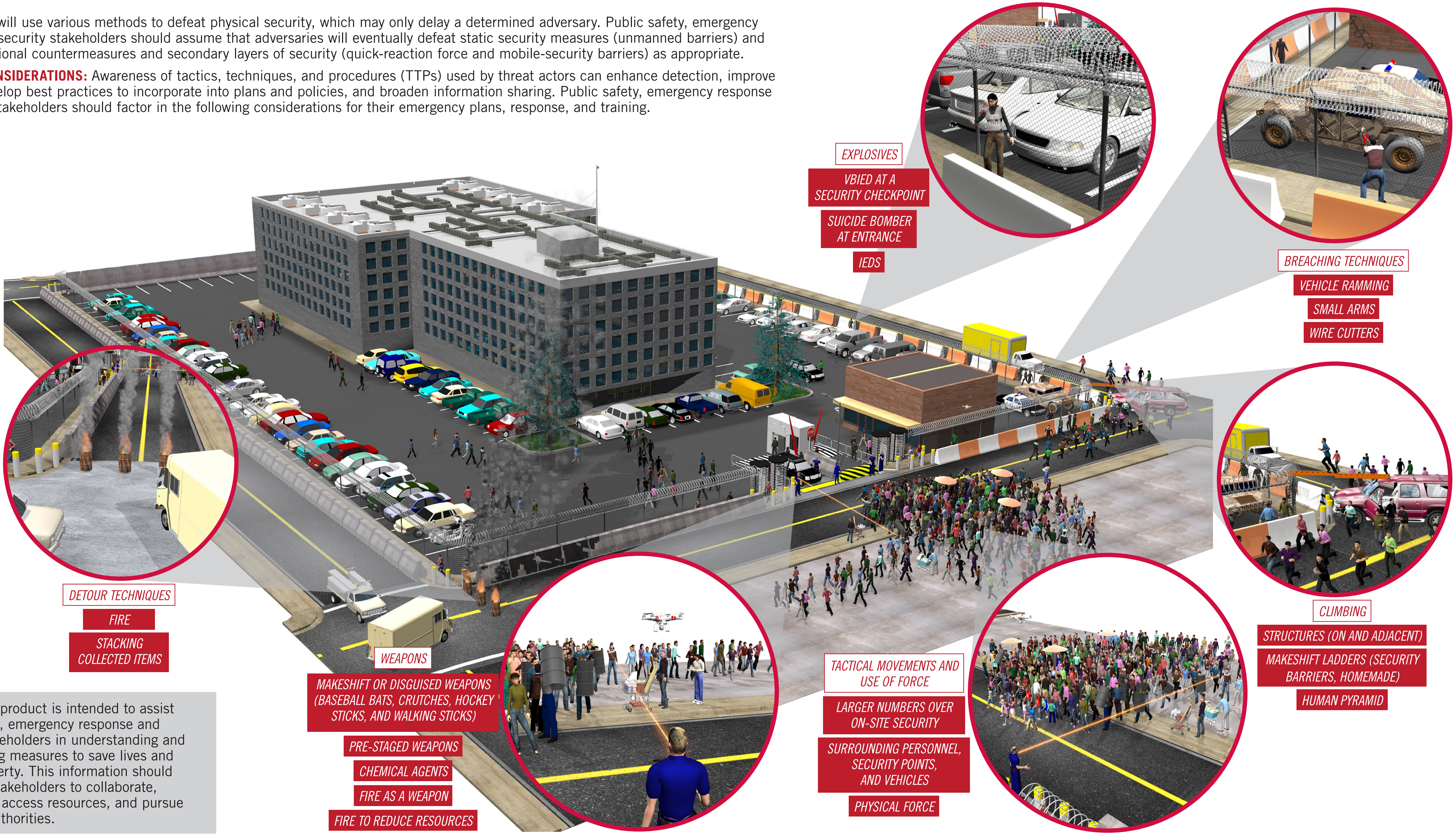
FIRST RESPONDER'S TOOLBOX

NCTC

Awareness of Violent Extremist Tactics To Defeat Physical Security Can Improve Response

Threat actors will use various methods to defeat physical security, which may only delay a determined adversary. Public safety, emergency response and security stakeholders should assume that adversaries will eventually defeat static security measures (unmanned barriers) and consider additional countermeasures and secondary layers of security (quick-reaction force and mobile-security barriers) as appropriate.

RESPONSE CONSIDERATIONS: Awareness of tactics, techniques, and procedures (TTPs) used by threat actors can enhance detection, improve response, develop best practices to incorporate into plans and policies, and broaden information sharing. Public safety, emergency response and security stakeholders should factor in the following considerations for their emergency plans, response, and training.



EXPLOSIVES
- VBIED AT A SECURITY CHECKPOINT
- SUICIDE BOMBER AT ENTRANCE
- IEDS

BREACHING TECHNIQUES
- VEHICLE RAMMING
- SMALL ARMS
- WIRE CUTTERS

DETOUR TECHNIQUES
- FIRE
- STACKING COLLECTED ITEMS

WEAPONS
- MAKESHIFT OR DISGUISED WEAPONS (BASEBALL BATS, CRUTCHES, HOCKEY STICKS, AND WALKING STICKS)
- PRE-STAGED WEAPONS
- CHEMICAL AGENTS
- FIRE AS A WEAPON
- FIRE TO REDUCE RESOURCES

TACTICAL MOVEMENTS AND USE OF FORCE
- LARGER NUMBERS OVER ON-SITE SECURITY
- SURROUNDING PERSONNEL, SECURITY POINTS, AND VEHICLES
- PHYSICAL FORCE

CLIMBING
- STRUCTURES (ON AND ADJACENT)
- MAKESHIFT LADDERS (SECURITY BARRIERS, HOMEMADE)
- HUMAN PYRAMID

SCOPE: This product is intended to assist public safety, emergency response and security stakeholders in understanding and implementing measures to save lives and protect property. This information should encourage stakeholders to collaborate, seek advice, access resources, and pursue additional authorities.

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, the FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies or procedures. For additional information contact us at JCAT@NCTC.GOV. **This document is best printed in 11 X 17.**

NCTC 037664 ID 9-21

17 SEPTEMBER 2021
AUTHORED BY NCTC, DHS, AND FBI

Awareness of Violent Extremist Tactics To Defeat Physical Security Can Improve Response *(continued)*

TYPES OF TACTICS THREAT ACTORS MAY USE TO OVERCOME OPERATIONAL OR PHYSICAL SECURITY MEASURES

Coercion or Duress	Using influence through mental pressure (bribery or blackmail) or threatened violence against a person (employee or security personnel) to facilitate hostile access into a facility.
Deception or Impersonation Technique	Assuming the identity, behavior, or appearance of another to blend into a surrounding environment, gain access to selected targets, or confuse responding security forces. This can include the use of "official" badges, identifiable vehicles (first responders, military, federal or local government agencies, public utilities, or other private sector entities), nameplates, rank insignias, uniforms, or unit identification to permit access to a selected target. Examples include: • The occupant(s) of a vehicle may use pretense to gain facility access. This can include the use of deception (lies, forged or stolen documents) or disguises to appear genuine or confuse and distract security personnel. • Unknowing mule: The use of a person (delivery driver or employee) to unknowingly deliver attackers, hidden firearms, IEDs, or weapons into a protected area.
Encroachment	Using a hostile vehicle to potentially exploit gaps by rural or urban landscape or perimeter protection; driving slowly through or over what is perceived to be a perimeter or series of obstructions; or closely tailgating a legitimate vehicle through a single-layer vehicle-access control point.
Insider	A current or former employee or person with regular access to a facility who provides information or materials to violent extremists. Insiders may or may not actively participate in the attack and are a constant security vulnerability. Violent extremists have used insiders to facilitate and conduct attacks and view them as valuable assets for obtaining information, gaining access, exploiting vulnerabilities, and challenging security countermeasures.
Parking	Parking a vehicle (legitimately, illegally, or without consent) close to an asset or inside the perimeter of a facility. The vehicle may be parked repeatedly to create familiarity, appear abandoned or unoccupied for short or long periods before a potential attack, or parked unsecured within or outside of a protected area and may be used by the attackers.
Penetrative	Using a vehicle to breach or weaken security measures. This type of attack may involve the use of an IED detonating close to security barriers to create a gap in physical security measures to allow follow-on hostile vehicles to enter a crowded area. A low-speed attack may involve a vehicle being aggressively and repetitively rammed against security barriers to gain access.
Sabotage or Tamper	With the intent of leaving no evidence, this type of attack can facilitate hostile vehicle access later. This may involve altering, weakening, or disabling a barrier or associated security systems. In addition, this type of attack can include an aggressive physical attack against barriers—at or just before—to facilitate a fast-moving attack or a physical or cyber attack gradually over time or immediately before an attack.

Best Practices

Information Sharing, Response, and Training

- Develop strong and effective security measures through joint planning and information sharing.
- Maintain situational awareness outside the incident perimeter, and monitor for similar threatening or suspicious activities beyond the target area.
- Prohibit parking in restricted areas (emergency access roads, staging areas, along fence lines or other sensitive locations).
- Establish pedestrian buffer and vehicular exclusion zones outside the fence line to engage threat actors before they get too close.
- Practice working within the buffer zone to maintain the standoff distance and to limit accessibility to targets by threat actors.
- Ensure security-response plans include 24/7 standby repair crews, with dedicated protective security while they conduct repairs.
- Threat actors may target perceived softer targets outside the secured zone, such as local businesses.
- Investigate suspicious purchases, loss or theft of law enforcement, fire service, emergency medical service and other emergency and security stakeholder branded items (agency patches, jackets, shirts, and uniform items) to mitigate their use by threat actors.
- Secure unattended emergency vehicles; establish a policy for decommissioning vehicles that makes them difficult to use unlawfully; establish familiarity with the types, makes and models of vehicles used by neighboring jurisdictions and supporting agencies; use difficult to replicate identifiers on emergency vehicles, such as holograms; and issue "be on the lookout" warnings for high-interest or suspicious vehicles.
- Develop well-defined rules of engagement, establishing appropriate security perimeters around the incident site(s), to include monitoring bystanders, and controlling egress and ingress routes.
- Make targeted arrests for federal crimes, whether they can be made contemporaneously with the commission of the crime or not.

Physical Security

- Assess fencing in and around the perimeter of the potential target and reinforce weak points, including by welding, adding weighted barriers (concrete or plastic), and installing base plates.
- Conduct routine inspection of fenced areas, and frequently inspect such areas for damage or partial breaches.
- Secure or remove adjacent structures.
- Consider the placement of cameras in key locations. Capturing seemingly innocuous or suspicious activity can be helpful in identifying, arresting, and prosecuting suspects.
- Install alternate surveillance systems, such as pole cameras or unmanned surveillance systems in case of destruction or failure of primary surveillance systems.
- Position larger and heavier response vehicles to restrict access to unauthorized personnel.
- Use flame retardant paint on wooden structures.
- Stage fire hoses for emergency use by responding personnel.
- Wear and inspect personal protective equipment (eyewear, gloves, helmet, vest) for effective use against bodily fluids, hard objects, lasers, and other toxic substances.

Threat Actor TTPs

- Use of vehicles that appear to have a legitimate purpose to transport and stage objects near the target, such as construction materials (barrels, crates or pallets), to negotiate fences and barriers.
- Use of improperly installed or unsecured fencing as barricades against responding personnel.
- Physical damage, destruction or obstruction (paintball guns or spray paint) to surveillance systems to hide unlawful activity.
- Use of lawn equipment (leaf blowers) to redirect deployed pepper or tear spray back to law enforcement officers.
- Use of innocuous objects (squeeze bottles or water balloons) to spread surreptitiously accelerants as a diversion or primary attack mechanism.
- Use of miscellaneous objects (furniture, makeshift spike strips, or vehicles) to create roadblocks, restrict responder access, disable emergency vehicles, or provide threat actor cover.

RESOURCES

DEPARTMENT OF COMMERCE

- **Facility Security Assessments** is an in-depth analysis used to determine security measures needed to protect Departmental personnel, property, and information in accordance with Interagency Security Committee (ISC) risk management process standards. https://www.commerce.gov/osy/programs/physical-security/facility-security-assessments

DHS

- **Guide to Conducting a Physical Security Assessment of Law Enforcement Facilities** provides an overview for analyzing and assessing the physical security posture of a law enforcement facility. Please contact NUSTL@hq.dhs.gov for document access.
- **ISC Agency and Facility Compliance Benchmarks** can be used to help federal security professionals implement security policies and mandatory standards. To request access, please send an email to ISCAccess@hq.dhs.gov with your full name and contact information, including email, agency name, and reason for access to this document.
- **Nonprofit Security Grant Program** provides funding support through the Federal Emergency Management Agency for target hardening and other physical security enhancements and activities to nonprofit organizations that are at high risk of terrorist attack. https://www.fema.gov/grants/preparedness/nonprofit-security
- **Physical Security Training Program** is a Federal Law Enforcement Training Centers' introductory physical security training program designed to provide baseline knowledge of physical security systems and procedures as defined by ISC guidelines. https://www.fletc.gov/training-program/physical-security-training-program

DEPARTMENT OF VETERAN AFFAIRS (VA)

- **Physical Security and Resiliency Design Manual** (revised 1 April 2021) contains the baseline physical security and resiliency requirements for improving the protection of Mission Critical Facilities, Life-Safety Protected (LSP) Facilities, and LSP Facilities with MC Utilities/Systems Redundancies of the US Department of VA. https://www.cfm.va.gov/til/PhysicalSecurity/dmPhySec.pdf

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) product. JCAT is a collaboration by NCTC, DHS, the FBI, and state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The product promotes coordination among intergovernmental authorities and the private sector in identifying, preventing, and responding to terrorist activities. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies or procedures. For additional information contact us at JCAT@NCTC.GOV. **This document is best printed in 11 X 17.**

JOINT
COUNTERTERRORISM
ASSESSMENT
TEAM
JCAT

PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: □ LE □ FIRE □ EMS □ HEALTH □ ANALYSIS □ PRIVATE SECTOR DATE:

PRODUCT TITLE: Awareness of Violent Extremist Tactics To Defeat Physical Security Can Improve Response

POOR ○ ○ ○ ○ ● GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT