

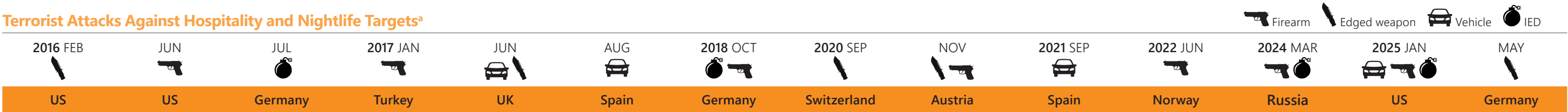
Tailored Security for Major Events Mitigates Terrorist Threat to Hospitality and Nightlife Industry



SCOPE: This product was coauthored by the Joint Counterterrorism Assessment Team (JCAT) and Canada's Integrated Threat Assessment Centre (ITAC) with contributions from the Scottsdale Police Department. The intent is to emphasize mitigation strategies that enhance collaboration between public safety and private-sector partners during major events. Although a number of the attacks highlighted in this graphic did not occur during a major event, we include them to demonstrate that terrorists continue to perceive this industry as a viable soft target. This product is not a response to a specific terrorist threat.

Proximity to or association with major events create unique security and planning challenges for hospitality and nightlife venues, including bars, nightclubs, restaurants, and cafes. Such venues remain attractive terrorist targets probably because of their association with particular targeted communities, easy access, and high occupancy levels. The venues' relatively limited security measures make them vulnerable to low-sophistication attack methods, which have few observable indicators and require little to no training. Al-Qa'ida and ISIS media outlets have long called for like-minded supporters to attack soft targets using weapons such as knives, vehicles, and edged weapons. Group-level messaging does not usually indicate an imminent attack but rather is designed to instill fear and spur lone offenders' plotting, although online violent extremist content on its own rarely mobilizes readers to violence. Other disruptive tactics, such as reporting hoax emergencies, offer low-cost, low-risk ways to cause panic, encourage violence, and drain and divert law enforcement resources.

Terrorist Attacks Against Hospitality and Nightlife Targets^a



Mitigating Common Attack Tactics

By taking into consideration some of the most common tactics used to target the hospitality, entertainment, and nightlife industry and then planning, coordinating, and training against them, stakeholders will be better prepared to prevent, respond to, and mitigate the effects of terrorist attacks.

Lone offenders using **edged weapons**—such as knives, machetes, and box cutters—and **firearms** remain a persistent threat to hospitality and nightlife venues and in some cases are able to avoid detection until they are ready to attack.

- Maintain a visible security presence, especially during peak venue/event operating hours.
- Implement appropriate access control measures, such as bag checks or screening for prohibited items.

- Mandate regular staff training about reporting suspicious behavior to reinforce the importance of proactive security measures and incident responses.

Terrorists often use **vehicles** to target pedestrians, breach venue physical security barriers, and deliver explosive devices.

- Layer spaced barriers, block adjacent sidewalks, and space approaching vehicles out to prevent piggybacking.
- Restrict access or limit speed with bends, serpentines, and offset approaches; use traffic-calming measures; and enforce standoff distances between potential targets, vehicle security barriers, and authorized parking.

Arson and improvised incendiary devices can be used against crowded nightlife and entertainment locations, although terrorists in the United States and Canada have not incorporated them frequently into their attacks.

- Develop an emergency action plan with local fire and emergency medical service (EMS) personnel, addressing access to fire-control and -suppression materials, first aid stations, triage areas, fire and EMS vehicle staging, and emergency ingress/egress routes.
- Define the perimeters between areas that require pedestrian and vehicle access control and those that require special access controls, such as control and computer server rooms and areas housing HVAC and other mechanical equipment.

Terrorists in the United States and Canada are most likely to use **unmanned aircraft systems (UAS)** against mass gatherings through reconnaissance (flying over the event), disruptive activities, or dropping weaponized payloads. Spotters may accompany UAS pilots in an attempt to counter security measures, making it difficult for public safety officials to see or hear UAS within certain distances of the target depending on the type of UAS.

- In the event of a downed UAS, contact qualified individuals to handle the flight data recoverable through forensic extraction techniques or by referencing the SD card when recovering the UAS; do not attempt to power the device on, because it may lead to the loss of data.
- Consider using UAS for protective security measures, such as providing elevated surveillance of blind spots, rooftops, and concealed or restricted areas.

 **JCAT First Responder's Toolboxes** provide information about terrorist tactics, techniques, and procedures and response and mitigation considerations and can be found on [JCAT's website](#).

- [Awareness of Preoperational Surveillance Tactics Associated With Terrorism Offers Opportunities](#)
- [Large Public Gatherings Attractive Targets for Violent Extremists](#)
- [Third-Party Security Critical to Safeguarding Public Gatherings From Terrorist Threats](#)
- [Evaluating and Responding to Violent Extremist Hoax Threats](#)

- [Vehicle-Borne Attacks: Tactics and Mitigation](#)
- [Terrorist Attacks against Bars, Restaurants, and Nightclubs Worldwide Highlight Importance of Public and Private Sector Partnerships in the Homeland](#)
- [Terrorist Messaging Urges Use of Edged-Weapons](#)

NCTC-DHS-FBI: [US Violent Extremist Mobilization Indicators booklet](#)

^aPeople who are affiliated or collaborating with foreign violent extremists directed, enabled, inspired, or otherwise conducted these attacks. In some cases, the hospitality or nightlife venue may not have been the primary target but was easily accessible or adjacent to outdoor or other mass gatherings.

Tailored Security for Major Events Mitigates Terrorist Threat to Hospitality and Nightlife Industry *(continued)*

Considerations

Security planners should tailor their approach on the basis of crowd size, location, venue, threat environment, and resources available to meet partner needs.

Physical Security: Address some facility security gaps with the following protective measures:

- Ensure CCTV cameras or video systems are operable and monitored appropriately.
- Conduct site walk throughs for multidisciplinary stakeholders (even those familiar with the venue) to identify and resolve concerns, particularly because event-related security and access modifications may alter the scene and affect accessibility, communications, and response.
- Collaborate with rideshare services to establish specific dropoff and pickup zones; advertise the zones through signage, on-site announcements, and messaging on social media and event websites.
- Use stanchions, barriers, chains, or ropes to limit the number of people at ingress/egress points.
- Light the facility adequately, and conduct routine visual security checks.
- Increase law enforcement presence during peak operating hours or during specific events.
- Limit, relocate, or lock items that can be thrown or conceal IEDs, such as trash containers, away from crowds or critical infrastructure.
- Implement screening measures when feasible, such as bag checks and personnel and weapons screening.
- Provide floorplans to law enforcement, fire, and other emergency responder agencies prior to an incident or major event through enhanced collaboration and networking.
- Consider scanning the ID documents of patrons entering nightlife or hospitality facilities and watching for visible anomalies or discrepancies indicating possible fraudulent documentation. These actions may indicate criminal or terrorist activities when combined with other suspicious behaviors.

Planning: Promote information sharing before a major event—or an emergency situation—by developing relationships between law enforcement, businesses, and communities of interest in the area. Establish and update a counterterrorism (CT) awareness and emergency response plan that addresses the following elements:

- Response protocol in specific threat event scenarios, such as a bomb threat or suspicious package or device
- Roles, responsibilities, and managing personnel for the entirety of an incident
- Evacuation
- Physical security checks and a search protocol, including daily checks incorporated into the routine maintenance schedule
- Staff training schedule, including new employee and refresher training and specialized training for staff assuming new responsibilities
- Accessibility of pre-staged first aid equipment
- Unified platform to maintain communications between public safety officials and private-sector partners during routine operations and events
- Emergency communications plan, including assigning responsibilities for working with law enforcement, fire, and EMS personnel and handling media requests

Third Parties: Hospitality and nightlife venues routinely host outside independent contractors, such as third-party vendors, promoters, DJs, sound and light technicians, and delivery personnel, who may have unique accesses to or knowledge of the facility. Consider conducting background checks, standardizing credentials, and implementing entry screening processes, such as metal detectors, for these people.

Impersonation of Uniformed Personnel: Malicious actors may impersonate government, military, law enforcement, fire, or other official personnel while trying to conduct reconnaissance or gain access to restricted areas or public officials. Although many of these instances are likely in support of criminal activities, they can also be part of plotting and executing a terrorist attack during major events.

Indicators

Venue employees, contractors, volunteers, and third-party personnel are uniquely positioned to identify behaviors reasonably indicative of terrorist or criminal activity. The activities listed below may be innocent, so support any determination of illicit intent with additional facts. However, when observed in combination with other suspicious behaviors—particularly advocating violence—the following indicators may constitute a basis for reporting:

- Unusual interest in or avoidance of security and access control measures and assets, such as personnel, hours and peak times of operation, entry points, CCTV systems, alarms, doors, gates, locks, and evacuation procedures
- Reporting hoax emergencies, such as bomb threats, to observe security and law enforcement responses
- Out-of-place items, such as empty or used packaging or materials for explosive precursors, in trash or other areas
- Loitering, parking, or standing in the same location for an extended period of time or on multiple occasions with no reasonable explanation
- Significant changes in physical appearance or attempts at disguise between repeated visits

Resources^b

Regularly train staff on general CT awareness and the venue's emergency response plan. Although not inclusive, the following resources are available online:

-  [Cybersecurity and Infrastructure Security Agency \(CISA\) commercial facilities sector information](#)
-  **CISA active-assailant security resources:**
 - [Physical security active shooter preparedness information](#)
 - [Physical security bombing prevention information](#)
-  [CISA Violence Prevention Through De-escalation video](#)
-  [Nationwide Suspicious Activity Reporting \(SAR\) Initiative \(NSI\) Private Sector Security training](#)
-  [American College of Surgeons Stop the Bleed campaign](#)
-  **Federal law enforcement training:** Contact the active-shooter coordinator or private-sector coordinator at the [local FBI field office](#) with questions.
 - The FBI [Active Shooter Attack Prevention and Preparedness](#) course prepares partners to prevent and respond to an active shooter.
 - [Advanced Law Enforcement Rapid Response training](#) prepares law enforcement to neutralize an active-shooter threat, control the scene, and provide initial emergency medical care.
-  [Royal Canadian Mounted Police \(RCMP\) National Security Information Network tip reporting form](#)
-  [Canadian Police Knowledge Network Active Shooter/ Armed Intruder Awareness Training course](#)
-  [Canadian Association of Chiefs of Police/ Counter-Terrorism and National Security Committee Countering Violent Extremism Guidebook](#)
-  [British Columbia RCMP Emergency Alert information](#)
-  [Public Safety Canada: Countering Crime](#)

 Training/resources offered by US  Training/resources offered by Canada

^bThe materials listed illustrate the variety of offerings and should not be considered endorsements of the content offered.

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@ODNI.GOV. This document is best printed on 11"x17" paper.



PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

<https://www.JCAT-url.com>

For further information, please email JCAT
jcat@odni.gov



(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.