**White Paper: The Hostile Event Attack Cycle (HEAC), 2021 Update**

*Developed by David Pounder and Andy Jabbour, Gate 15, with an introduction by Rob Yandow*.

**Introduction**.

A basic understanding of the **Hostile Events Attack Cycle** (**HEAC**) is a critical element in the development of a functional and effective plan to prepare for, and perhaps prevent, a hostile attack against an individual, group, or physical facility. This white paper, as presented by Gate 15, provides an excellent analysis of the various components of the HEAC by identifying and describing each stage of the Cycle along with the progressive steps that attackers could take in furtherance of their goal which is to perpetrate violence against their selected target(s). The paper also identifies the important connection between the Hostile Events Attack Cycle and the Pathway to Violence. I will undoubtedly incorporate the information contained in this white paper into future safety and security discussions at all levels.

**Rob Yandow**, Retired Police Captain

National Sector Chief

InfraGard Emergency Services Sector

**The Hostile Event Attack Cycle (HEAC), 2021 Update**.

Looking across the threat spectrum, hostile events can take the form of many types and their impacts on individuals, organizations, and community can be far-reaching, and, in a lot of ways, devastating. They can incorporate many different types of threats. These include[[1]](#footnote-1) active shooter incidents, workplace violence and workplace attacks, lone actor and low-tech terrorism, complex coordinated terrorist attacks, fire as a weapon, weapons of mass destruction, and other related hostile actions. And they are characterized by several factors, and employed through a variety of means, weapons, and tactics used to cause physical injury or death. Regardless of the attack method, hostile events present an operational range of hazards requiring a more complex response strategy that blurs the lines between traditional law enforcement, fire, and emergency medical service (EMS) duties and responsibilities. Whether they realize it or not, threat actors go through a cycle for planning and executing an attack. This process is defined as the Hostile Event Attack Cycle, or HEAC, and it is based on a review of various attacks, as well as other articles based on various types of attack processes[[2]](#footnote-2)[[3]](#footnote-3).

***The purpose of this paper is to provide an understanding of the HEAC which can help organizations prepare for various threat courses of actions and develop enhanced security measures as necessary to potentially disrupt threat actors’ planning and to enable the organization to be prepared to respond appropriately.***

In early 2016, The Gate 15 Company (Gate 15) consolidated several existing concepts and developed the HEAC model. This was shared amongst information sharing and analytical communities, and other security professionals, and subsequently informed the basis of Gate 15’s hostile events preparedness program (the Hostile Events Preparedness Series [[HEPS](https://gate15.global/services/heps/)]). Initially eight phases, this level of understanding about the threat and their planning process provided insight to organizations to potentially counter threat activities and reduce the risk to their organization. However, as more attacks were analyzed, some consolidation to the HEAC has occurred. While the actions within the phases are distinct, there are instances in which actions bleed together and do not necessarily follow a chronological order. Additionally, with the abundance of information available to threat actors online and through social media platforms, threat activities can be expeditated and done in conjunction with physical activities.

They HEAC process merges several important concepts and publications from within the public and private sector.

* At the foundation is a basis developed through observed active shooter instances[[4]](#footnote-4) which include five distinct stages: Fantasy; Planning; Preparation; Approach; and Implementation.
* The individual elements which include the outer and inner blocks of the cycle correspond to the Pathway to Violence[[5]](#footnote-5) and FBI[[6]](#footnote-6) information and analysis which incorporate Grievance, Ideation, Planning and Research, Breach, and Attack.
* As a result, HEAC can be viewed as seven phases, represented in the chart below.

Diagram, schematic

Description automatically generatedBy utilizing this process, threat actors have a framework, again whether followed consciously or not, in which they select the best target to satisfy their purpose; that they have the right supplies and equipment; and then once the attack is over, that they conclude the attack as intended – via an escape or death. Whether it is a physical attack designed to inflict mass casualties, or an attack on facilities or infrastructure, the HEAC is consistently followed as threat actors plan, prepare, and execute their attacks.

A couple points to consider in reading this report:

* The term threat actor used throughout this document applies to an individual or group.
* When evaluating hostile events, we make a clear distinction between these events (as defined above) and crimes of passion, in which an act is committed against another because of sudden strong impulse such as sudden rage, rather than as a premeditated crime. Hostile Events discussed in this report may be conceived based on a grievance but are not impulse driven; they are not spur of the moment decisions. This does not discount that the impulse or source of that impulse does not factor into the target selection, but it is not the sole factor in committing the act.
* In a similar vein to the above, the hostile events described through the HEAC are different from other criminal incidents that may be called active shooter incidents but in fact related to criminal violence, or other type of activity such as gang-related, or narcotics incidents.

**Fantasy Stage.** This includes the Initial Target Considerations, and Initial Surveillance / Research phases. Within this stage, the threat actor likely knows that they want to commit a hostile event, but is not clear on when or where. Thus, they need to work through that process – identify the potential targets, conduct research to whittle down their list based on opportunity, and potential security challenges.

**Phase 1 – Initial Target Considerations.** This is the act of identifying potential targets based on the threat actor’s beliefs, ideology, or their perceived grievance. The goal of this phase is to identify the purpose and objectives for the attack. In the initial planning stages of an attack, the threat actor will consider many targets based on, or influenced through, a multitude of factors that could include personal beliefs, inspiration from extremist groups, terrorist organizations or individuals in the way of propaganda, or through a reaction to an event in their life (triggering event). As part of the process to whittle those choices down, the threat actor will need to identify which target represents the best opportunity to achieve their desired end-state, whether that is to inflict a desired amount of damage and bring notoriety to themselves or their cause.

Initial target considerations can come about from several different ways.

* **Ideological.** A threat actor may select a target based on their upbringing and their core beliefs. This can often be associated specifically with religious based teachings and influences, but it can also apply to other types of [extremist groups and beliefs](https://www.fbi.gov/cve508/teen-website/what-are-known-violent-extremist-groups), such as White Nationalism, Animal Rights groups, or even Anti-Abortion groups. In October 2020, six men [were arrested and charged](https://www.justice.gov/opa/pr/six-arrested-federal-charge-conspiracy-kidnap-governor-michigan) federally with conspiring to kidnap the Governor of Michigan. According to a complaint the FBI began an investigation earlier in the year after becoming aware through social media that a group of individuals was discussing the violent overthrow of certain government and law enforcement components. This group used operational security measures, conducted coordinated surveillance on the Governor’s vacation home and discussed various weapons and training activities to prepare for the attack.
  + In November 2019, a 16-year-old girl was [arrested for planning to attack](https://www.nbcnews.com/news/nbcblk/16-year-old-girl-allegedly-plotted-attack-black-church-georgia-n1086196) and kill members of a church in Gainesville, Georgia. The church was targeted based on the racial demographic of the members, who were predominantly black.

In a May 2021 [joint report](https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view), the FBI and DHS note that the greatest terrorism threat to the Homeland today is posed by lone offenders, often radicalized online, who look to attack soft targets with easily accessible weapons. Many of these violent extremists are motivated and inspired by a mix of socio-political goals and personal grievances against their targets.

Threat actors are easily adaptable and equally influenced by current events. In 2020, they sought to exploit the COVID pandemic, while in 2021, they attempted to exploit the easing of COVID-related restrictions. Using various platforms, ideologically-motivated extremists fueled by perceived grievances, false narratives, and conspiracy theories continue with the intent to incite violence.

* + In the March 2019 attack on a mosque in Christchurch, New Zealand, the threat actor gave [insight](https://www.aljazeera.com/news/2019/03/zealand-terrorist-attack-suspect-grins-court-190316011147796.html) into his motivation behind the attack through his manifesto in which he “identified himself by name and said he was a white supremacist who was out to avenge attacks in Europe perpetrated by Muslims.” The [manifesto in full](https://observer.news/assets/The-Great-Replacement.pdf) went into detail, albeit rambling at times, about immigration, population control, and white genocide, but at the root of it was his desire to strike at what he views as the invasion of Islam and their “high fertility rates” that are used to “grow to replace peoples and faith”.
* **Grievances.** In a series of studies on active shooters, the FBI has defined [grievances](https://www.hsdl.org/?view&did=812282) as “the cause of the active shooter’s distress or resentment; a perception — not necessarily based in reality — of having been wronged or treated unfairly or inappropriately.”
  + In 2018, a man [killed five members](https://www.capitalgazette.com/news/crime/ac-cn-capital-shooting-hearing-1028-20191028-nkxc5ukn4nbzjdwoltewbmqx6u-story.html) of the Capital Gazette newspaper staff stemming from a harassment case filed against the man and were reported by the Capital Gazette in a 2011 column.
* **Stressors.** Various studies have correlated stress to criminal behavior. Similar to grievances, the FBI [identifies](https://www.hsdl.org/?view&did=812282) these as “physical, psychological, or social forces that place real or perceived demands/pressures on an individual and which may cause psychological and/or physical distress.” However, while there may be grievances that add to stress, stressors are pressures or concerns related to their interpersonal relationship with family, friends, or co-workers, financial pressures, or some sort of action in their life that is applying pressure to the point where the individual must act.
  + Examples of stressors resulting in hostile events are evident in some workplace violence incidents. For example, there may be individuals who lose their jobs and may decide to take action. In February 2019, a man [killed five fellow employees](https://chicago.cbslocal.com/2019/04/29/gary-martin-henry-pratt-shooting-report-police-justified/) in Illinois after he was told he was being fired for a safety violation. Apparently, hours before, he allegedly threatened “If I get fired, I’m going to kill every mother f\*\*\*\*\* in here” and the threat actor was known to have had a gun in his car, though no one had ever seen him with the weapon inside the warehouse.
* **At the Direction of a Larger Group (Influenced / Inspired).** This could be considered a sub-set of ideology, but there are attacks that are planned at the direction of a larger group, such as a terrorist or extremist group. An individual will belong to that group, but in this case is more of a follower and only takes direct action at the request of the group leadership.
  + The gunman in the December 2019, Pensacola Naval Air Station shooting [was found](https://www.nytimes.com/2020/05/18/us/politics/justice-department-al-qaeda-florida-naval-base-shooting.html) to be “regularly in touch with Al Qaeda for years, including the night before the attack.” The FBI found that the man, who was a Saudi Air Force cadet training with the American military “had communicated with leaders of Al Qaeda in the Arabian Peninsula and had joined the Saudi military to carry out a ‘special operation.’”
  + In October 2020, a French teacher was beheaded walking home from school after one of his recent classes studied freedom of expression in the context of the *Charlie Hebdo* Muhammad cartoons. Days after the attack, “The Voice of Hind,” a monthly magazine released online by ISIS supporters in India, [ran a full-page graphic](https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-magazine-publishes-photo-of-french-teachers-head-calls-for-more-attacks-on-free-expression/) urging more attacks and incorporating a photo of the severed head of the French teacher.
  + In September 2020, two people standing outside of *Charlie Hebdo’s*former office were [attacked](https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-aqap-calls-for-attacks-preceded-stabbings-outside-former-charlie-hebdo-office/) with a meat cleaver and survived the assault. This was in response to the magazine’s decision to republish the controversial cartoons depicting the Prophet Mohmmed in advance of the trial of the [2015 Charlie Hebdo attack](https://www.bbc.com/news/world-europe-30708237).

**Phase 2 – Initial Surveillance / Research.** In this phase, the threat actor will gather information about potential targets that ensure it will meet the objectives of the attack. The goal now is to reduce the number of potential targets while recognizing that additional information requirements about the target are still outstanding. It is not important that the threat actor makes their selection during this phase, but they will have accumulated enough information to aid in that decision.

In order to accomplish this, the threat actor will identify basic background information about each potential target and identify questions that need to be answered prior to ultimately selecting a target. This research can be done through a variety of means, but will most likely start off with online searches through various social media platforms or a target’s website. Once that research is done, the threat actor will need to validate that research through physical target surveillance. However, it should also be noted that while physical surveillance is preferred, there may be some targets and opportunities where physical reconnaissance will not be possible and the threat actor will therefore have to rely solely on virtual surveillance. This is one reason why organizations and individuals should be careful as to how much information they provide online. The more posted online, the more potential threats are able to glean to facilitate their process.

Initial surveillance is the first time that the threat actor will go out and physically observe the potential target(s) in the context of this specific act. They may already be familiar with the target location (as discussed below) but may not have considered the security elements they would need to factor in when planning their attack. The [main objectives](https://protectioncircle.org/2013/06/14/the-hostile-planning-process/) of initial surveillance are to validate the information already collected through open-source research, identify and collect new information not available through research, and to eliminate potential targets prior to settling on a final target.

This surveillance allows the threat actor to confirm what their research has shown and to identify areas that could not be learned through this research, such as physical facility security. Through direct “eyes-on” surveillance, the threat actor can get a first-hand look at the outward facing security (i.e., guard posts, security patrols) and countermeasures (i.e., identification card checks, bag checks or other screening measures). If the target of the attack is a person or group, the threat actor may use surveillance to monitor routes to and from various locations - i.e., home to work, work to regular meeting sites, or to detect common travel patterns the target takes. The threat actor may draw maps or diagrams of target locations and continue to refine and refocus further collection.

A threat actor can utilize several different methods to conduct this surveillance.

* ***Mobile*** surveillance in which the threat actor follows the target, or drives by the target via foot, or vehicle.
* ***Static, or fixed point****,* surveillance in which the threat actor observes from one location, i.e., an observation post outside a target location.
* ***Online*** surveillance – learning about the target through analysis of their online footprint, i.e., websites, social media, etc.
* ***Aerial*** surveillance which incorporated drones to discreetly follow a target or surveil a fixed location. Aerial surveillance can be considered part of mobile or static surveillance, it is also important to single it out as a separate area to signify the emerging threats and planning and preparedness consideration of drones.
* The threat actor can use one or another of these methods but good surveillance incorporates more than one approach to learn as much as possible.

***Surveillance of a target does not always have to be done strictly at the target site***. For example, the [Manchester concert bombing attack](https://apnews.com/hub/manchester-concert-bombing) in 2017 happened at a sports arena, and while the threat actor wanted to know as much as possible about this one specific arena, for this type of attack, specific details may not have been necessary. Threat actors can also use similar types of locations to identify potential vulnerabilities. Recognizing that arenas will follow similar protocols in their security plans (why reinvent the wheel, right?), the threat actor could have done surveillance in other locations or venues. In the Manchester attack, it was later revealed in the [official government inquiry](https://manchesterarenainquiry.org.uk/?gclid=Cj0KCQiA_qD_BRDiARIsANjZ2LBVMC3GTpN2bNbQgOrKsPaBIPm48Ob2tit0SLh_3IiO2Yg6sriV5V4aAt1kEALw_wcB) that the threat actor did in fact conduct an extensive level of surveillance in support of his plan. Nevertheless, organizations should recognize that **the threat is present even if not at their specific location**.

The act of surveillance does not need to be a covert activity wherein an individual or group strictly hide in proverbial bushes. The threat actor may use others or unwitting individuals to help surveil or collect information against a target. They may use social engineering or elicitation techniques to engage unwitting employees to pull out information about important times for security changes, or security measures within the facility. The threat actor could also co-opt employees to serve as their eyes and ears and help the planning process. Every employee, whether they were a parking attendant, retail worker, or house cleaning, has information that can aid a threat actor.

[Social Engineering:](https://searchsecurity.techtarget.com/definition/social-engineering) Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain.

[Elicitation](https://www.macmillandictionary.com/us/dictionary/american/elicitation): the process of getting information from someone. In a security context, elicitation is done discreetly or without knowledge of the intent.

Threat actors can also conduct surveillance as part of their normal day-to-day activities, such as going to the mall, or visiting a tourist location. They will know the target simply because they have seen it enough to know. Additionally, terrorist and extremist groups provide advice and information regarding targets in their communications channels or in propaganda to help threat actors understand without necessarily having to conduct extensive physical surveillance. In the 21 July 2019, El Paso shooting, the threat actor took a slightly different approach for planning and executing his attack. In his online manifesto, the threat actor revealed he might struggle with deciding whether to carry out the attack or not. As a result, he had formulated the plan, ensured he had all the weapons and equipment necessary to carry it out and then went to conduct [surveillance (casing)](https://abcnews.go.com/US/death-toll-rises-22-el-paso-shooting-victims/story?id=64780680) in the process of executing that attack. He already had his [manifesto written](https://www.nytimes.com/2019/08/03/us/patrick-crusius-el-paso-shooter-manifesto.html), and only needed to find the “right” location. Once he was satisfied with the potential targets inside, he was able to retrieve his weapon from his vehicle and initiate the attack. During that timeline he published his manifesto crossing a line he did not turn back from.

Other such examples include:

* The driver of an SUV that [plowed through a Chicagoland mall](https://nypost.com/2019/09/20/suv-leaves-trail-of-destruction-after-plowing-into-illinois-mall/) in 2019 obsessively researched the center online prior to the mayhem that sparked more than 100 terrified calls to 911. In the day before his attack, that threat actor [conducted 124 internet searches](https://nypost.com/2019/09/30/chicagoland-mall-terrorist-did-obsessive-research-before-attack-prosecutors/) on Woodfield Mall in suburban Schaumburg, including the stores inside and street and aerial views, prosecutors said in Leighton Criminal Court on Sunday.
* In the 2019 New Zealand attack, the threat actor visited the mosques in Christchurch and Linwood, when he ultimately decided to change his plans. According to his manifesto, “The Christchurch and Linwood mosques had far more invaders, in a more prominent and optically foreign building, with less students, more adults and a prior history of extremism.” The third mosque on his list was in Ashburton where the mosque was a converted church which he viewed as “the desecration of the church.” When the threat actor was ultimately stopped by police at the conclusion of the attack, it is believed he was on his way to [continue his attack there](https://www.newshub.co.nz/home/new-zealand/2019/03/christchurch-terror-attack-the-gunman-s-next-target.html), which is an hour’s drive from Linwood.

Depending on the target, some key examples of what intense surveillance will want to determine include, but are certainly not limited to:

* Target is a Person:
* Confirm daily schedule – to and from work, after work activities, weekend activities.
* Does target vary travel patterns?
* Identify known associates.
* Identify locations the target frequently visits; what is the level of security at those locations.
* Target is a Location:
* What are the layers of security outside and inside the location; are their roving patrols on foot by security personnel or vehicle patrols; how often and how many people are involved?
* Does the facility have external surveillance platforms?
* Does the facility have a receptionist or check in area; what is that like?
* Are there alternate entrances that are not secure?
* Does the facility have a loading dock or delivery area; what is that security like?
* How often are deliveries made and on what schedule?
* What is the security response to suspicious events or materials?

**Planning Stage.** This stage includes the Target Selection phase and sets the foundation for the rest of the hostile event. Based on the development during the Fantasy Stage and first two phases, the threat actor makes the decision on the target and in doing so transitions from a mere concept in the threat actor’s mind closer to reality and officially kicks off the detailed planning of the attack.

**Phase 3 – Target Selection.** During this phase, the threat actor ultimately selects the target of that attack. The threat actor will take the information gathered to this point and make a decision on the specific target(s). The initial surveillance and research conducted to this point will help the threat actor identify the target that offers the greatest chance of success based on available information. The threat actor will be able to identify when the attack could occur, the type of security, and the amount of impact the attack will have.

This process can take time and the threat actor may also identify targets unintentionally. In the New Zealand attack, that threat actor’s manifesto noted that he began “planning an attack roughly two years in advance and an attack at the location in Christchurch three months in advance… The attack was planned to allow enough time to train, form a plan, settle my affairs, write down my views, then enact the attack.” New Zealand was not the original choice for the attack, as he “only arrived to New Zealand to live temporarily whilst [he] planned and trained,” but he soon found out that New Zealand was not only as good of a location as anywhere else in the West, but also that New Zealand would show that nowhere in the world was safe, and that “the invaders were in all of our lands, even in the remotest areas of the world.”

**Preparation Stage:** This stage includes the ever-important Planning and Rehearsals (Surveillance). Now that the target has been identified, it is now necessary for a more deliberate portion of the planning. In the Fantasy Stage, the threat actor did preliminary work which included research on the target. Now, that research will need to be more developed and in-depth, which could include periods of intense physical surveillance, building out and finalizing plans based on the information developed, and rehearsals.

**Phase 4 – Planning and Rehearsals (Surveillance).** This is the phase in which the threat actor will finalize the plan to exploit potential vulnerabilities and weaknesses identified in earlier actions. This phase will also incorporate additional surveillance and rehearsals to finalize the plan, though these actions may be unstructured, disjointed, and informal. At the end of this phase, the attack plan should have been developed and the threat actor will work to complete the acquisition of needed supplies and equipment, if this hasn’t been done throughout the planning to date.

There are several actions that go into finalizing the plan:

* Building upon the initial surveillance, the phase will include **additional surveillance** which will go into more detail and could involve a lot more “time on target,” or time that is spent observing and getting to know the target in-depth. This allows the threat actor to learn as much as possible and help build the attack plan and lock down any unknowns to make sure the attack can accomplish the goals.
  + This was seen recently in September 2020, Charlie Hebdo attack in which the threat actor allegedly [made two reconnaissance](https://www.thenationalnews.com/world/europe/pakistani-immigrant-charged-over-charlie-hebdo-knife-attack-1.1086293) visits in the days leading up to the attack yet, still had no idea Charlie Hebdo had moved locations, which indicates not enough initial surveillance was done. Even so, the threat actor still carried out an attack despite not having positive confirmation or conflicting information about the true location of the target.
  + In the October 2020, in the [Michigan plot](https://www.hstoday.us/subject-matter-areas/infrastructure-security/the-hostile-events-attack-cycle-in-the-militia-plot-to-kidnap-michigan-governor/) (in which a group attempted to kidnap the Governor of Michigan), the threat actors conducted an extensive amount of planning and surveillance, specifically visiting the target site on multiple occasions, including at night, to survey the environment as well as assess escape routes, and to plan for responding law enforcement activities.
* Taking all the information developed to date, the threat actor will formalize the plan and begin to **build the various phases of the attack** – pre-attack, to include logistics planning; actions at the target; and post-attack (escape/evasion/death).
* Once the attack planning has taken place, it will be necessary for the threat actor to **rehearse the plan** - especially the key elements - in order to ensure they can properly execute the plan. This can be accomplished in a manner similar to a drill, an exercise, or using scalable models, which is a more advanced method. If possible, a scaled mockup would be beneficial to the threat actor to rehearse properly. The individuals in the Michigan kidnapping and attack plot [held a training event](https://www.justice.gov/opa/pr/six-arrested-federal-charge-conspiracy-kidnap-governor-michigan) at a member’s property in which they worked on constructing and testing an explosive device that would be used in the attack. These rehearsals will help the actor(s) identify potential issues. This may also cause the threat actor to go back and conduct additional surveillance or change the plan slightly which could be a good opportunity to identify indicators of a potential attack.
  + Familiarity with the target will have an impact on this as it did with surveillance. So, whether the rehearsal is a full-scale model, or a mental walk through, reviewing and rehearsing the plan often takes place.
  + For some attacks, the rehearsal can simply be firing and familiarity with a weapon system and reloading. In the 2015 [Charleston, South Carolina Church shooting](http://www.cbsnews.com/news/dylann-roof-charleston-church-shooting-prosecutors-give-timeline-actions/) the planning and rehearsals included the threat actor firing his weapon and reloading it at various outdoor locations and in his backyard. The threat actor had a good understanding of the target – he visited the site, and made phone calls to the location to gather information. Weapons training was effectively the one remaining element needed to rehearse for success.

Depending on the size of the attack and the number of threat actors, there may be formalized or informal planning meetings to discuss the specific details of the attack. Referencing back to the [Michigan plot](https://www.justice.gov/opa/pr/six-arrested-federal-charge-conspiracy-kidnap-governor-michigan), the individuals met several times in smaller, sometimes one-on-one meetings, as well as in larger groups.

A rehearsal can address the entire plan, focus on one specific phase of the attack, or even work on an area that may need extra work. The threat actor In the 2015 [Charleston, South Carolina Church shooting](http://www.cbsnews.com/news/dylann-roof-charleston-church-shooting-prosecutors-give-timeline-actions/) rehearsed firing his weapon and reloading it at various outdoor locations and in his backyard. Weapons training was effectively the one remaining element needed to rehearse for success.

Some of the planning considerations during this phase are listed below:

* **Pre-Attack Planning:**
  + Of critical importance is ensuring the threat actor has the right tools, equipment, and weapons available to accomplish the task, or at least to develop a way to acquire those.
  + Logistics planning will also include how the threat actor will arrive, and whether or not the threat actor will need to escape and evade law enforcement.
* **Attack Planning:** 
  + The threat actor will need to identify how to approach the target and how to leave the target location. If the target is a building or facility, then he will also need to determine how the threat actor will enter and exit (a building, a fenced-in area, etc.). This is where surveillance is critically important. The threat actor will need to know what obstacles / security could be in the way of their objective and how to defeat those obstacles.
  + The threat actor will need to ensure they have the best chance to accomplish their mission so depending on the attack method, they will need to ensure that they know where they are going and where to set up the attack.
  + If the attack involves multiple people, they will each have assigned roles and responsibilities. The attack planning will finalize this and assign tasks.
  + The threat actor will also need to identify the expected response from security and outsiders and consider possible variables that may impact accomplishing the task.
* **Post-Attack Planning:**
  + Much of this depends on whether the threat actor intends to give their life in order to inflict as much damage and casualties as possible, or if the threat actor intends to escape and evade security / law enforcement.
  + If survival is a consideration, then some escape and evasion considerations will incorporate disposal of equipment and weapons.
  + An additional planning consideration is whether a support network is used to help the escape and the plan for leaving the immediate area.

**Approach Stage.** This stage includes the Pre-Attack Operations Phase and takes the threat actor right to doorstep of the attack. This phase represents the time in which the threat actor will ensure all the supplies, equipment, and tools are obtained and prepared for that attack.

**Phase 5 – Pre-Attack Operations.** During this phase, the threat actor will ensure all the supplies and equipment are ready for the attack. This represents the last time before the attack to ensure the plan and supplies are in good order and positioned for the attack. This phase is one of the more flexible elements of the HEAC as the threat actor will focus on ensuring all the equipment, weapons, and logistics for the attack are prepared and ready. Equally important is that each threat actor will start to focus on their own internal preparation in order to get mentally prepared for what is to come. This represents a small, but unique vulnerability for alert and aware bystanders to key in on, and by doing so may be able to disrupt potential attacks by being attune to behavioral changes.

This phase gives the opportunity for the threat actor to review the target, review all the notes and planning considerations, and to get all the equipment needed for the attack and consolidated in one area. These Pre-Attack Checks (or Pre-Combat Checks or Inspections using military terminology) are the chance to check to make sure all the major pieces, or equipment, needed for the successful completion of the attack are accounted for, are functioning, and ready for the attack. This includes individual equipment as well as team equipment, such as vehicles. Some of the checks that threat actors will review:

* Individual:
  + Weapons accounted for and functioning.
  + Specialty gear necessary for the attack on hand and working; this can include cameras and other type of streaming equipment that has been used in some recent attacks to document and “memorialize” the attack for followers.
  + Plans reviewed and verified to include individual actions at the target site.
  + Escape plans reviewed and verified.
  + Water and food on hand and packed, if necessary.
  + First Aid gear.
* Team / Group:
  + Plans reviewed and verified to include individual actions at the target site.
  + Escape plans reviewed and verified.
  + Dry run / map rehearsal of actions at the target site.
  + Vehicles working.
  + First Aid available and packed.
  + Communications devices working between team members.
  + Equipment checked and loaded.
* When pre-attack operations are not successful, threat actors may not realize the full success of their planned attack. The [New York City Subway attack](http://www.cnn.com/2017/12/11/us/new-york-possible-explosion-port-authority-subway/index.html) on 11 December 2017, represents one such instance. The threat actor had a plan, he executed the plan, and yet at the moment of attack, the device [did not work as expected](https://www.cnn.com/2017/12/11/us/new-york-possible-explosion-port-authority-subway/index.html). While there were some injuries, the threat actor suffered the most and additional damage and destruction was averted. It is possible that the threat actor did not do his necessary checks prior to the attack, or that he did not test the device to know that it would have worked when needed.

**Implementation Stage.** This stage includes the Attack and the Escape phases. It begins when the threat actor has completed their pre-attack checks and is ready to initiate the attack. This represents the culmination of all the work done by the threat actor to succeed. Related to the escape, this is a phase that may not be part of every attack plan. For some, the attack will be the final act, while others may make the attempt to escape, though analysis shows that escapes are rarely, if ever successful.

**Phase 6 – Attack.** Put simply, this is the physical act of carrying out the attack plan and is the culmination of the HEAC. All the planning and preparations that were undertaken by the threat actor will go into a moment that will define both the threat actor and target. A successful outcome for the threat actor when going through the HEAC is that the attack accomplishes its goals and the threat actor either attempts to escape or accepts the outcome of the attack and surrenders or continues the attack against responding law enforcement or security elements. While the preparedness and response of the target have a large part in how successful an attack may be, from the adversary’s end, the success of the attack will be directly tied to the amount of planning and preparations made.

* Did the threat actor understand the security situation?
* Did the threat actor accomplish their goal?
* Did the threat actor do what was necessary to ensure success?

The outcome of the attack, or even getting to the point of initiating the attack, will also depend on the manner in which the preparation was done. Specifically, did the threat actor practice good operational security (OPSEC) in their actions, and were they able to effectively reduce the number of vulnerable times or indicators that others could have picked up on and reported potential suspicions to authorities. As recently as September 2020, the threat actors [planning the kidnapping of the Governor of Michigan](https://www.justice.gov/opa/pr/six-arrested-federal-charge-conspiracy-kidnap-governor-michigan) were undone by poor OPSEC and a clandestine source. In May 2020, an individual from Tampa, Florida was [arrested for providing material support to terrorist groups](https://www.justice.gov/opa/pr/tampa-man-charged-attempting-provide-material-support-isis) and possibly planning an attack in public spaces in the Tampa area after revealing suspicious indicators to associates who reported it to authorities. Time and time again, attacks are disrupted or degraded when individuals and organizations report suspicious activities and behaviors. If the threat actor is going to be successful, not only will the planning and preparation have to be properly conducted, but it must be securely conducted as well.

**Phase 7 – Escape.** This is the act of evading responding law enforcement and security teams from the scene of the attack. While the escape is a phase within the cycle, it is not a phase that will be carried out by all threat actors and in many instances, this will be determined early in the HEAC process. For example, threat actors who carry out attacks based on ideology or a belief system may determine that the manner of their attack will mean that they sacrifice their life for their beliefs (i.e., suicide bombing), or continuing the attack until all weapons and ammunition are used and mass causalities are produced. These threat actors will accept that their calling will be to sacrifice their life in the execution of the attack and in an effort to make it as lethal as possible.

In other types of attacks, however, the threat actor may plan for the escape, but will not be able to complete that action. There are several reasons why an escape, even planned, may not always work out. For example:

* An escape may require extra surveillance, coordination, and logistics which may add extra layers of complexities that could be identified as suspicious or concerning, or;
* This extra layer of planning for an escape may introduce a new level of uncertainty in the attack preparation phases and could increase the risk of compromise or disruption.

***A threat actor cannot completely plan for the response from first responders, security elements, or eyewitnesses/bystanders,*** making any such planning and preparation difficult and time consuming. For example, and threat actor can conceivably have a plan for escape but can’t very easily conduct a rehearsal realistically replicating similar conditions, or events. In the 2013 Boston Marathon bombing, the threat actors fled the scene with the intent of conducting additional attacks. Ultimately, the threat actors carjacked a vehicle and [set off a series of events](http://www.chicagotribune.com/news/nationworld/chi-boston-marathon-bombing-trial-20150316-story.html) they could not have planned or anticipated for, which led to one threat actor’s death and the subsequent arrest of the other.

Another immeasurable factor in planning an escape is the ***adrenaline rush*** that accompanies an attack. After the attack, the threat actor will likely experience an emotional high with a big adrenaline spike. However, if not trained for, the rush can lead to mistakes. According to [Psychology Today](https://www.psychologytoday.com/blog/threat-management/201001/adrenaline-rushes-can-they-help-us-deal-real-crisis), “With a big hit of adrenaline, we tend to lose situational awareness. Our brains perceive danger and prepare us for ‘fight or flight.’ We lose our peripheral vision and focus on what is right in front of us. Our brain works to filter out any sound extraneous to the direct threat (auditory exclusion). We hyperventilate or hold our breaths. In some instances, this is exactly what we need to get out of harm’s way, but in many intense situations, we need to be able to think clearly, hear what people around us are saying, breathe deeply to send oxygen to our brains, and act effectively to be able to survive the situation or master the skill we are learning.”

Finally, a consideration for threat actors is that many escapes may not result in success. Some may not even try.

* The threat actor in the 2015 Berlin Christmas Market attack fled through the Netherlands before traveling to Italy where he was ultimately killed. Authorities believe his escape was an [attempt to evade detection](http://www.telegraph.co.uk/news/2016/12/28/german-police-arrest-alleged-contact-christmas-market-killer/), and thus highlights a level of forethought and planning.
* Dylann Roof, the threat actor behind the 2015 massacre of a black church in Charleston, South Carolina clearly [did not plan for an escape](https://www.charlotteobserver.com/news/local/article24952345.html) but left the scene and drove away, heading to Nashville because “he had never been there before.” He made no efforts to conceal his travel and put up no resistance when pulled over and arrested.
* In the 2015 San Bernardino attack in which 14 people were killed by a couple influenced by the Islamic State, the threat actors [made their escape](https://legal.thomsonreuters.com/en/insights/case-studies/san-bernardino) in a rental vehicle before switching to another vehicle. It didn’t make a difference as law enforcement was able to track their activity, ultimately executing a traffic stop that led to a shootout and the death of both threat actors.

And as mentioned above, in some attacks, escapes are simply not part of the plan, or death is viewed as the final escape, and is never a consideration as part of the attack. Depending on the threat actor’s moral, ethical, or religious views, death may be viewed as the ultimate achievement in support of their beliefs. And in other situations, such as workplace violence murder-suicides, death may be the escape from events in their life or the event that pre-empted the violence.

**MITIGATION**. Depending on the attack method, prevention can vary. For lone actor attacks such as Dylann Roof, or [Nidal Hasan](https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Nidal%20Hasan.pdf) (the convicted killer at Fort Hood), and with individuals who are isolated or ostracized within their community, it can be difficult to disrupt their planning. However, there are some common indicators of an individuals’ movement towards violent action that can be detected and provide opportunities to frustrate plots and prevent tragedy. **By following a routine attack cycle (whether they are aware of it or not) individuals expose themselves to detection and disruption**. Some of these exposure points provide windows of opportunity, albeit limited in most cases, for security elements or members of an organization to identify and report the suspicious activity. Individuals, who may be in a position to spot indicators of this type of activity can create a series of events that could lead to disruption of a larger attack.

Training and awareness of how various threat actors think and identifying unusual/suspicious behavior is a fundamental task for organizations. This process should involve legal and human resource elements, but ultimately front line personnel – employees, volunteers, or whomever is likely going to make first contact with potential threats - are the first line of defense. While organizations may vary on size, leadership and security elements can only observe through a limited prism and may be focused solely externally. Employees can help serve as external sensors that can note suspicious activity outside the office, and also internally, potentially identifying Insider Threats or potential work-place violence incidents in advance.

**Practice Security Mindfulness. Know yourself – could you be a target?**

* Has your business or an individual associated with your business been engaged in activity that may cause them to be a target for one reason or another. They may represent an ideological target based on their business model or their public comments. They could engage in practices that may have a negative impact on a particular ethnic group or religious belief. For example, simply being identified as “Jewish”, “Muslim”, “conservative”, or “anti-environment” could have a negative impact on an organization.
* Have they produced a product that resulted in a high number of customer complaints or issues? Whatever the business, it is recommended to do a thorough assessment of themselves to identify if there are any issues that may increase the likelihood of an attack against the facility or individuals connected with the building.
* Are there any associated risks? Even if the business may not be a target, there could be associated risks based on a number of factors. For example, in an election season, politicians may make public visits in order to appeal to voters which may make not only the politician a potential target, but those locations where the politician visits a potential target. Additionally, tenants of buildings could make the entire facility a target potentially exposing other individuals or businesses to increased risk.
* Coordinate with neighbors and local law enforcement to understand the potential threats in and around your area. Because demographics and situations may change, it is important to maintain this contact to ensure your information is up to date.

**Know the Threat.** Recognize the threats and their capabilities. Have there been previous attacks on your organization directly, or on the like facilities? What type of capabilities do potential threat actors have? What other attacks have occurred against other like entities (by critical infrastructure sector, geographic location, etc.) or targets that may be applicable?

**Operational Security.** Understanding operational security, and protecting sensitive information, is a key element for protecting against surveillance. This includes security of buildings, facilities, parking lots, and associated properties, as well as online elements including public facing websites and social media platforms. Recognizing the importance of providing information to prospective customers from a business standpoint, organizations should look to reduce the amount of detail about people and places. This increases the amount of information the threat actor needs to acquire about the target and could potentially reduce the chance of attack.

**Behaviors.** Depending on the attack method, prevention can vary. For lone actor attacks and with individuals who are isolated or ostracized within their community, prevention can be extremely difficult. However, there are some common indicators of an individuals’ movement towards violent action that can be detected and provide opportunities to frustrate plots and prevent tragedy. According to a recent FBI analysis, “Each bystander in a person of concern’s sphere represents an opportunity to identify potential warning behaviors.”[[7]](#footnote-7) Behavior supports assessments as to the appropriate level of concern and guides management strategies.While some attacks are thwarted at the “last second,” security personnel, supported by a trained and aware workforce, have the opportunity to detect and interdict plots before they reach the lethal attack phase.

Throughout the HEAC, the threat actor may recognize the finality of their upcoming actions and decide to take part in activities that they would not normally do. The New Jersey Office of Homeland Security and Preparedness [noted](https://www.njhomelandsecurity.gov/analysis/new-jersey-familys-report-thwarts-pressure-cooker-bomb-plot) that “family members, peers, and close contacts may be the first to notice radical shifts in behavior and attitude, as well as unusual Internet activity.” This was after a family **member notified law enforcement of someone’s erratic behavior. The man was arrested and charged with** plotting to build a pressure-cooker bomb and detonate it in New York City to “kill as many people as possible” in support of the Islamic State.

In the 09 November 2020, NCTC First Responder’s Notebook, “[*Bystanders Are Key to Countering Terrorism*](https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/102s_-_First_Responders_Toolbox_-_Bystanders_Are_Key_To_Countering_Terrorism-survey.pdf)” they note, “Family, peers, community leaders (religious figures, teachers, coaches, work supervisors), and strangers are all examples of bystanders who may observe suspicious behaviors reasonably indicative of terrorism or criminal related activity. **To enable disruption of attacks, bystanders must understand the important role they play in terrorism prevention and the available opportunities to report pertinent suspicious information.**”

The shifts in behavior may also manifest in various ways. Some individuals may withdraw, or withdraw further, from their friends and family; others may begin to engage in reckless behavior knowing that their outcome is predetermined; others may look to establishing or re-establishing a connection with religion; while others may seek to reconnect with lost friends or family or wrap up personal matters. Some individuals may start giving away cherished personal effects or items to those closest to them without much explanation. These shifts are not necessarily things that may not happen abruptly or immediately before the act, but can occur over a period of time, with some happening immediately and beforehand.

Finally, for some threat actors, this Pre-Attack Operations period can create vulnerabilities. Some threat actors may get jittery and feel compelled to visit the target location or unnecessarily validate their surveillance with one final run through. The [Nice, France terrorist threat actor](http://www.telegraph.co.uk/news/2016/07/17/nice-terror-attack-police-vans-blocking-promenade-withdrawn-hour1/) drove through the area in the same truck he would use to kill over 80 people two days later, scrutinizing locations and evaluating the best place to execute his attack, in addition to going through a period of time using drugs and engaging in unusual sexual behavior. This type of suspicious behavior by the threat actor created two potential vulnerabilities that may have been pieces of information that authorities could have used in a larger puzzle.

**Pathway to Violence.** During this planning process, and especially right before the attack is initiated, the individual(s) involved in the attack may start to withdraw as they come to grips with what is to come. They may start to pull back from family and friends; they may become more agitated; or post troubling statements online through social media or in passing conversations with others. Two resources can help organizations with training on suspicious behaviors or activities.

* CISA’s [Pathway to Violence](https://www.cisa.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf) document
  + Be Alert to Signs of Trouble: Potential warning signs include:
    - Increasingly erratic, unsafe, or aggressive behaviors.
    - Hostile feelings of injustice or perceived wrongdoing.
    - Drug and alcohol abuse.
    - Marginalization or distancing from friends and colleagues.
    - Changes in performance at work.
    - Sudden and dramatic changes in home life or in personality.
    - Financial difficulties.
    - Pending civil or criminal litigation.
    - Observable grievances with threats and plans of retribution.
  + Appropriate Intervention. Help ensure the safety of you and your colleagues by:
    - Being aware of drastic changes in attitude toward others.
    - Taking note of any escalations in behavior.
    - Providing any information that may help facilitate intervention and mitigate potential risks.
  + Reach Out for Help. Contact your supervisor or your human resources department to alert them of potential dangers and enable them to mitigate any emerging risks.
  + [Pathway to Violence Video.](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiJ9cS-pPTsAhXG1FkKHVrVC4YQFjAAegQIBBAC&url=https%3A%2F%2Fwww.cisa.gov%2Fpathway-violence-video&usg=AOvVaw0HOeVdIjL2u-L-rIqca-KB) This video is a training aid that provides information regarding the behavior indicators that assailants often demonstration before a violent act. This video also describes the six progressive steps (similar to the HEAC process) that may be observable by colleagues.
* The “[If You See Something, Say Something](https://www.dhs.gov/see-something-say-something/recognize-the-signs)” campaign. This infographic provides observable activities that could be indicators of potential threat-based activities that would support the HEAC.

**Security Briefings / Information Sharing.** Incumbent upon knowing the threat is developing information sharing relationships internally and externally. Security organizations should ensure that all employees are aware of the potential threats so they can be prepared in the event of an incident. Externally, information sharing exchanges about threats and threat tactics between organizations will ensure better preparedness and development of plans. This should include industry groups, such as Information Sharing and Analysis Centers (ISAC) and Organizations (ISAOs), community security groups, relationships with local fusion centers and law enforcements, and other appropriate formal and informal groups. Reach out to local neighbors and law enforcement to enhance understanding and coordination regarding threats and response.

* Threat briefings are an important part to helping employees recognize behavior patterns and should be a part of a regularly scheduled interval. These briefings should not just focus on nation-state sponsored, or terrorist inspired attacks. These should include active shooter and workplace violence attacks. Case studies and field studies by law enforcement organizations are excellent training aids to help train employees and alert them to warning signs.
* In addition, several existing programs are available to organizations to help prevent these types of attacks; the US Department of Homeland Security advocates “See Something, Say Something” while the U.S. Army has established a Threat Awareness and Reporting Program. These programs both work to provide training to employees on behaviors as well as to give people an outlet for reporting suspicious behavior. Additional training and references include:
  + Indicators of an individual’s movement towards violent action. DHS has developed several sites with useful reference material organizations can access to help inform security awareness efforts including Active Shooter focused sites (see [here](https://www.dhs.gov/active-shooter-workshop-participant), and [here](https://www.dhs.gov/active-shooter-preparedness)) and a website focused on [Countering Violent Extremism](https://www.dhs.gov/publication/countering-violent-extremism-resources) and regarding “[Hometown Security](https://www.dhs.gov/hometown-security).” Gate 15 has also consolidated [additional resources online](https://gate15.global/resources/) that can help organizations in their planning and preparedness.
  + [The Power of Hello](https://www.cisa.gov/employee-vigilance-power-hello). Simply saying “Hello” can prompt a casual conversation with unknown individuals and help you determine why they are there. The OHNO approach – Observe, Initiate a Hello, Navigate the Risk, and Obtain Help – helps employees observe and evaluate suspicious behaviors, and empowers them to mitigate potential risk, and obtain help when necessary. The [CISA Power of Hello Slick-sheet](https://www.cisa.gov/publication/power-hello-resources) and [CISA Power of Hello Placemat](https://www.cisa.gov/publication/power-hello-resources) provides organizations with information to assist in identifying and effectively responding to suspicious behavior.
  + Crisis Management and Communications teams should work together to provide employees and vendors with a “What to Communicate” and “What not to Communicate” sheet to reduce and minimize threats.
  + Reinforce security education and drills. Short, “hip-pocket” overviews that can be taught in limited time windows, can remind employees, and especially help part-time or seasonal employees, to focus on the basics, such as identifying and reporting suspicious behavior.

**Training / Rehearsals / Exercises.**Once the plan is in place, it needs to be communicated down to every employee, discussed during training events, and rehearsed through drills and other exercises. Rehearsals and exercises are also effective tools in identifying potential weaknesses in the plan that can be worked out and improved upon. Organizations should build and rehearse an employee accountability plan. This plan is a low-cost measure that a company can take to ensure they capture one of the critical first steps in incident management and response. Build a plan; examine the plan and recommend changes; conduct occasional accountability drills across the organization; rinse and repeat. This plan should focus on immediate incident response accountability actions; engagement / interactions with first responders; and address company procedures and communications regarding unaccounted-for employees.

* **Run, Hide, Fight Training**. Regardless of the amount of planning and preparedness organizations go through to prevent or deter an attack, it is still necessary to train employees on how to respond should a hostile event occur. One of the models used is the Run, Hide, Fight model in the U.S. and similarly the Run, Hide, Tell model in the U.K. These models can help provide a foundation for employees to respond.
  + [FBI Run, Hide, Fight Video](https://www.fbi.gov/video-repository/run-hide-fight-092120.mp4/view)
  + [RUN. HIDE. FIGHT.® Surviving an Active Shooter Event - English](https://www.youtube.com/watch?v=5VcSwejU2D0&feature=player_embedded) (Video)
  + [Marauding Terrorist Attack (MTA): RUN. HIDE. TELL. - GOV.UK](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjeqKW3mqntAhVQu1kKHUpcAMkQFjAAegQIAhAC&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fcrowded-places-guidance%2Fmarauding-terrorist-attack-mta-run-hide-tell&usg=AOvVaw0AB1IpaSMayjvxli8WlLhG)

**Formalize the Security and Incident Response Plan.**One of the critical tasks within these phases lies in the incident response. Based on the threat, and each location, each organization should develop the appropriate plan to protect its people, facilities, and data. Additionally, how will each organization respond to a security incident / attack? It’s important that all employees and emergency responders, internal and external to an organization, have a copy of and an understanding of emergency plans.

**Employ Random Active Measures.** Random Active Measures are actions by security elements that are enacted “randomly” to throw off the cycle. They introduce an element of uncertainty for the threat actor. Threat actors will surveil during all hours in an effort to identify patterns and find the best time to conduct an attack. If this planning is disrupted by random security measures it may throw off planning and cause the threat actor to choose another target. Some examples include:

Gate 15’s **Hostile Events Preparedness Series (HEPS)** is intended to give organizations a **complete preparedness solution to addressing the threat of a hostile event**. Addressing threats such **active shooters, workplace violence, low-tech terrorism, complex, coordinated terrorist attacks** and related security concerns, our series of events – from education to full-scale exercises – can be conducted as individual activities or as a complete series, based on the needs and fit for each organization. Learn more about [**HEPS**](https://gate15.global/services/heps/).

* 100% ID Card and bag check.
* Making guard force change vary at different times.
* Adding pop-up barriers or new traffic patterns.
* Roving security patrols through parking lots or throughout the external parts of the building.
* Vehicle inspections.

**Report.** In line with CISA’s [Connect, Plan, Train, Report](https://www.cisa.gov/connect-plan-train-report) initiative, it is important to ensure that individuals and organizations share information. Specifically, CISA encourages organizations to contact law enforcement, but also to “Post details on reporting suspicious activity and encourage employees, tenants, and visitors to report suspicious behavior to property management security or local law enforcement. Things to consider include unattended vehicles; repeat visitors or outsiders who have no apparent business in non-public area; abandoned parcels, suitcases, backpacks, and packages; and other unusual activity.”

In addition, the NCTC’s First Responder’s Toolbox report (see callout box above) notes some important elements about reporting that organization are encouraged to consider:

* Reporting mechanisms that are secure, safe, anonymous, easily accessible, and credible likely will remove potential barriers and may increase bystander reporting.
* Providing multiple channels to share concerns with trusted interlocutors outside law enforcement—such as religious leaders or a community ombudsman—also could increase reporting rates, particularly among family members and peers who are the most hesitant to involve law enforcement.
* Developing intervening programs other than arrest for individuals at risk of committing terrorism or violence would probably encourage bystanders to report. Intervention programs typically use social workers, mental health professionals, employment and family counselors, and law enforcement personnel to develop individualized approaches to steer an individual away from violent extremism.

**PREVENTION IS NOT AND CANNOT BE A PASSIVE PROCESS.**

**HEAC Resources and References.** There were several links provided throughout the paper that served as either resources or references for organizations to utilize in their preparedness planning, or were used as examples of HEAC activity. Those items have been provided below for quick reference.

**Resources and References.**

* [Connect, Plan, Train, Report](https://www.cisa.gov/connect-plan-train-report) (CISA)
* [Run, Hide, Fight Video](https://www.fbi.gov/video-repository/run-hide-fight-092120.mp4/view) (FBI)
* [RUN. HIDE. FIGHT.® Surviving an Active Shooter Event - English](https://www.youtube.com/watch?v=5VcSwejU2D0&feature=player_embedded) (Video)
* [Marauding Terrorist Attack (MTA): RUN. HIDE. TELL. - GOV.UK](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjeqKW3mqntAhVQu1kKHUpcAMkQFjAAegQIAhAC&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fcrowded-places-guidance%2Fmarauding-terrorist-attack-mta-run-hide-tell&usg=AOvVaw0AB1IpaSMayjvxli8WlLhG)
* [Countering Violent Extremism](https://www.dhs.gov/publication/countering-violent-extremism-resources) (DHS)
* [Hometown Security](https://www.dhs.gov/hometown-security) (DHS)
* [Active Shooter Workshop – Participant Resources](https://www.cisa.gov/active-shooter-workshop-participant) (CISA)
* [Active Shooter Preparedness Resources](https://www.cisa.gov/active-shooter-preparedness) (CISA)
* [If You See Something, Say Something](https://www.dhs.gov/see-something-say-something/recognize-the-signs) (DHS)
* [Pathway to Violence](https://www.cisa.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf) – Warning Signs and What to Do Flyer (CISA)
* [Pathway to Violence Video](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiJ9cS-pPTsAhXG1FkKHVrVC4YQFjAAegQIBBAC&url=https%3A%2F%2Fwww.cisa.gov%2Fpathway-violence-video&usg=AOvVaw0HOeVdIjL2u-L-rIqca-KB) (CISA)
* NCTC First Responder’s Notebook: “[Bystanders Are Key to Countering Terrorism](https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/102s_-_First_Responders_Toolbox_-_Bystanders_Are_Key_To_Countering_Terrorism-survey.pdf)”
* [Surveillance Discussion](https://protectioncircle.org/2013/06/14/the-hostile-planning-process/) (Protection Circle)
* [A Study Of The Pre-Attack Behaviors Of Active Shooters In The United States Between 2000 And 2013](https://www.hsdl.org/?view&did=812282) (FBI)
* [Active Shooter Resources](https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources) (FBI). This page includes a number of additional reports on active shooter incidents and analysis.
* [Hostile Events Preparedness Series (HEPS) training](https://gate15.global/services/heps/) (Gate 15)
* [Strategic Intelligence Assessment and Data on Domestic Terrorism](https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view) (FBI/DHS)
* [Homegrown Violent Extremist Mobilization Indicators – 2019 (DHS)](https://www.dni.gov/files/NCTC/documents/news_documents/NCTC-FBI-DHS-HVE-Mobilization-Indicators-Booklet-2019.pdf)

**Hostile Event Examples.** The attacks listed below are an Index of the examples used in the paper.

April 2013 – [Boston (MA) Marathon Attack](https://www.cbsnews.com/news/dylann-roof-charleston-church-shooting-prosecutors-give-timeline-actions/)

January 2015 – [Charlie Hebdo (France) Attack](https://www.bbc.com/news/world-europe-30708237)

December 2015 – [Berlin (Germany) Vehicle Ramming Attack](https://www.telegraph.co.uk/news/2016/12/28/german-police-arrest-alleged-contact-christmas-market-killer/)

June 2015 – [Charleston (SC) Church Attack](https://www.cbsnews.com/news/dylann-roof-charleston-church-shooting-prosecutors-give-timeline-actions/)

May 2017 – [Manchester (England) Concert Bombing Attack](https://apnews.com/hub/manchester-concert-bombing)

December 2017 – [San Bernardino (CA) Attack](https://legal.thomsonreuters.com/en/insights/case-studies/san-bernardino)

December 2017 – [New York City Subway Attack](http://www.cnn.com/2017/12/11/us/new-york-possible-explosion-port-authority-subway/index.html)

June 2018 – [Capital Gazette Newspaper Attack](https://www.capitalgazette.com/news/crime/ac-cn-capital-shooting-hearing-1028-20191028-nkxc5ukn4nbzjdwoltewbmqx6u-story.html)

February 2019 – [Aurora (IL) Henry Pratt Company Attack](https://chicago.cbslocal.com/2019/04/29/gary-martin-henry-pratt-shooting-report-police-justified/)

March 2019 – [New Zealand Mosque Attack](https://www.bbc.com/news/topics/c966094wvmqt/christchurch-mosque-shootings)

September 2019 – [Chicago Vehicle Ramming Attack](https://nypost.com/2019/09/20/suv-leaves-trail-of-destruction-after-plowing-into-illinois-mall/)

November 2019 – [Georgia Church Plot](https://www.nbcnews.com/news/nbcblk/16-year-old-girl-allegedly-plotted-attack-black-church-georgia-n1086196)

December 2019 – [Pensacola (FL) Naval Air Station Attack](https://www.nytimes.com/2020/05/18/us/politics/justice-department-al-qaeda-florida-naval-base-shooting.html)

September 2020 – [Charlie Hebdo (France) Stabbing Attack](https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-aqap-calls-for-attacks-preceded-stabbings-outside-former-charlie-hebdo-office/)

October 2020 – [French Teacher Attack](https://www.dw.com/en/france-three-teens-charged-in-beheading-of-history-teacher/a-55526223)

October 2020 – [Michigan Militia Plot](https://www.justice.gov/opa/pr/six-arrested-federal-charge-conspiracy-kidnap-governor-michigan)

1. This definition is based on a variety of resources including the DHS Risk Lexicon, <https://www.cisa.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf>, the Interagency Board, <https://www.interagencyboard.org/sites/default/files/publications/External%20IAB%20Active%20Shooter%20Summit%20Report.pdf>, the US Secret Service, <https://www.secretservice.gov/sites/default/files/reports/2020-09/MAPS2019.pdf>, and US Federal Bureau of Investigation, <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources>, and others. [↑](#footnote-ref-1)
2. Scott Stewart, formerly with Stratfor, has written on the terrorist attack cycle, which HEAC expounds upon. Examples of that work include “[Stratfor on the Terrorist Attack Cycle](https://worldview.stratfor.com/article/stratfor-terrorist-attack-cycle)”, 03 Oct 2012, and “[The Terrorist Attack Cycle Remains Unbroken](https://worldview.stratfor.com/article/terrorist-attack-cycle-remains-unbroken)”, 27 Jul 2017. [↑](#footnote-ref-2)
3. DHS [Pathway to Violence](https://www.cisa.gov/publication/pathway-violence-fact-sheet) [↑](#footnote-ref-3)
4. [5 phases of the active shooter: A tactical reload](https://www.police1.com/active-shooter/articles/5-phases-of-the-active-shooter-a-tactical-reload-LWMMSAiCm4a51jek/) and [The 5 Stages of an Active Shooter](https://www.aig.com/content/dam/aig/america-canada/us/documents/business/industry/the-5-stages-of-an-active-shooter-brochure.pdf) [↑](#footnote-ref-4)
5. DHS [Pathway to Violence](https://www.cisa.gov/publication/pathway-violence-fact-sheet) [↑](#footnote-ref-5)
6. [Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks](https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Making%20Prevention%20a%20Reality%20-%20Identifying%20Assessing.pdf) [↑](#footnote-ref-6)
7. The Federal Bureau of Investigations. “Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks,” page 13. *The Department of Justice*. 2017. [↑](#footnote-ref-7)