

Threat Management *for the* **Lone Offender**



Federal Bureau of Investigation
National Center for the Analysis of Violent Crime
Behavioral Analysis Unit-1

Unclassified

Lone Offenders in the U.S.

Between May 31 and June 14, 2009, three lethal attacks were committed in different parts of the U.S. by individuals who had some connection to extremist ideology, but who acted alone. All three were male – and American – but their ideologies were different, their targets were different, and they did not conform to a single offender profile. This spate of incidents is a tragic reminder to law enforcement of the challenge posed by those referred to as “Lone Offenders,” “Lone Wolves,” and “Lone Terrorists.” Preventing these attacks is a Tier-1 priority for the FBI. This document previews an ongoing FBI study of these attacks, and offers some preliminary operational guidance for assessing and managing potential threats based on prior research and initial case observations.

FBI's Lone Offender Study

The FBI's Critical Incident Response Group (CIRG) Behavioral Analysis Unit (BAU) and Counterterrorism Division (CTD) Domestic Terrorism Operations Unit (DTOU) have initiated a collaborative research effort to study Lone Offender attacks to develop better knowledge and capacity to prevent them. In 2001, CTD commissioned the domestic Lone Terrorist Study, which contains some useful descriptive case information but did not systematically analyze attack-related behaviors.¹ The current FBI operational study builds upon that effort, aiming to better understand the processes of thinking and identifiable behaviors, which typically precede an attack or attempted attack, and to translate those findings into investigative guidelines. Findings and recommendations from the study will be distributed to FBI Field Offices, JTTF personnel, and other federal, state, and local law enforcement partners for operational use.

Lone Offender attacks are conceptualized in this study as a type of “targeted violence” – a term coined by Dr. Robert Fein and Bryan Vossekuil to describe “situations in which there is an identified (or identifiable) target and an identified (or identifiable) perpetrator.”² The attacks are premeditated and the targets generally symbolic of a particular ideology. The BAU and other experts who study these issues have observed similarities in the pre-attack behaviors of Lone Offenders and perpetrators of other forms of targeted violence, including assassins, some terrorists, as well as campus, workplace, and public place shooters. It can be difficult to define Lone Offender cases in a way that makes them distinct, but to provide coherence with CTD's mission, our behavior-based research effort has examined adjudicated cases meeting the following criteria:

- The act was conceived and executed by one or a few individuals not operating under the direction or influence of an organized group;
- While the subject may reach out to others for assistance, he/she is the primary architect of the operation, and his/her effort is self generated rather than directed by others;

¹ The Lone Terrorist Study publication (2001) is available on the CTD intranet site.

² Fein, R. A., & Vossekuil, B. (1998). Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials. Washington, DC: United States Department of Justice.

- The subject consciously accepts the use of lethal violence in furtherance of an ideological, political, social or religious cause; and
- The act resulted in homicide, or likely would have had unforeseen circumstances not occurred.

BAU has identified an initial sample of twenty-one offenders, and ultimately we hope to expand this into a more comprehensive “Targeted Violence” database.

The purpose of this document is not only to preview this study, but more importantly to provide behavioral tripwires and operational prompts for field personnel who must prioritize and manage investigations involving potential Lone Offenders. It should be noted that this study will not produce a “profile” of a Lone Offender. There are far too few (and disparate) offenders to create any definitive set of demographic or psychological screening criteria. Instead, the effort will emphasize the significance of the pre-attack *behaviors* that may come to the attention of law enforcement and others.

Learning from Prior Research on Targeted Violence

The BAU is modeling the Lone Offender research protocol after the U.S. Secret Service (USSS) Exceptional Case Study Project (ECSP).³ The ECSP – developed and led by Fein and Vossekuil – was the first operational exploration of the thinking and behavior of all 83 individuals known to have attacked, or approached to attack, a prominent public official or public figure in the United States since 1949. The behavior-based study included an examination of each subject's ideas and actions in the days and weeks before their attacks or near lethal approaches, focusing on what might be knowable to investigators or observers.

Researchers examined each subject's movement from the idea of the attack to the actual attack, including the subject's motives, selection of targets, planning, communication of threat and intent, symptoms of mental illness, and significant life experiences. In every case, the attack or near-attack was found to be the end result of an understandable (albeit disturbed and flawed) process of thinking and action. Given the nature of public figure assassination, the ECSP findings are inextricably intertwined with the Lone Offender issue. In fact, a number of the public figure attackers in the ECSP study had previously considered a Lone Offender-type attack. The findings are also relevant to security concerns about certain kinds of WMD-related attacks. ECSP findings heavily influenced this document, some key findings from the study are outlined below:⁴

Historical and Background Characteristics of ECSP Subjects:

- Most were described as social isolates. About a third were not.
- Many had histories of harassing other people.

³ Fein, R. & Vossekuil, B. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near lethal approachers. *Journal of Forensic Sciences*, 44, 321-33.

⁴ A full copy of the ECSP report is available through the USSS NTAC internet site.

- Most were known to have had histories of explosive, angry behavior, but only half were known to have been previously violent.
- Few subjects had histories of arrests for violent crimes or of incarceration.
- Most had histories of weapons use but lacked formal training.
- Most had interests in militant/radical ideas and groups but were not active members.
- Many had histories of serious depression or despair.
- Many are known to have attempted or considered suicide.
- Many had some contact with mental health professionals.
- Attackers were less likely than other approachers to have histories of delusional ideas.
- Few subjects had histories of command hallucinations.
- Few had histories of substance abuse, including alcohol.

Progression from Idea to Action:

- Many had problems coping in life and were feeling desperate and hopeless.
- Often subjects viewed the attack as a solution to some grievance or problem.
- Timeline for deliberation and planning ranged from weeks to years.

Motive:

- Motive generally was a major factor in target selection.
- Motives were often complex and multifaceted, including the following:
 - to achieve notoriety and fame;
 - to avenge a perceived wrong;
 - to end personal pain; to be killed by law enforcement;
 - to bring national attention to a perceived problem;
 - to save the country or the world;
 - to achieve a special relationship with the target;
 - to make money;
 - to bring about political change.

Planning:

- The extent of pre-attack planning ranged from slight to extensive.
- Most did not have technical expertise.
- The most careful planners were those whose motive was money.
- Less than a quarter had known escape plans.
 - About one third expected to die or wished to be killed.

Threats:

- Less than ten percent of all the assassins, attackers, and near-lethal approachers communicated a direct threat to the target or law enforcement agency.
- None of the successful assassins communicated a direct threat about their target to the target or to a law enforcement agency before their attack or near-lethal approach.

Mental Illness:

- Less than half of those who chose public officials or figures as their primary targets exhibited symptoms of mental illness at the time of their attacks or near-lethal approaches
- More of the subjects had some broadly-defined history of problems or symptoms
- Mental illness by itself is not a good causal explanation for targeted violence and may be misleading.

Operational Guidance: Threat Assessment⁵ & Targeted Violence

Threat assessment refers to a “set of investigative and operational techniques that can be used by law enforcement professionals to identify, assess, and manage the risks of targeted violence and its potential perpetrators.”⁶

Principles of Threat Assessment:⁷

- **Targeted violence – including lone offender attacks – are rarely sudden or spontaneous events.**
 - Targeted violence is the end result of an understandable, and oftentimes discernible, process of thinking and behavior.
 - Perpetrators don't “just snap.”
 - Successful attacks typically require some planning preparation relating to key activities such as targeting, discerning the proper time and approach, building capacity, and acquiring and transporting weapons.
 - The key lies in the identification of discrete attack-related behaviors to indicate a subject's movement along a pathway from thought to action.
- **Targeted violence stems from an interaction among the individual, the situation, the setting, and the target.**
 - Attacker: risk factors; development of ideas; preparatory behaviors; handling unbearable stress.
 - Situation: whether past events led to self-destructive or violent; how others are responding.
 - Setting: access, level of security.
 - Target: subject's familiarity w/ target; target vulnerability; target sophistication about caution.
- **A key to investigation and resolution of threat assessment cases is identification of subject's attack-related behaviors**
 - Effective threat assessment is based upon facts (observations of thinking and behavior), rather than subject characteristics or “traits.”

⁵ The term “Threat Assessment” as utilized in this document refers to the concept of behavioral threat assessment and should not be confused with relevant DIOG definitions pertaining to threat assessment.

⁶ Fein, R. A., Vossekuil, B., & Holden, G. A. (1995). Threat assessment: An approach to prevent targeted violence. National Institute of Justice Research in Action, 1-7.

⁷ Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17, 323-337.

- Discrete behaviors precede the attack.
- The continuum may include:
 - Idea > Communication > Inappropriate Interest > Research/Planning > Preparation > Approaching
- **An “integrated systems approach” should guide threat assessment inquiries and investigations.**
 - Using a team approach with information from varying sources and perspectives.
 - You may have only one piece of the puzzle.
- **The central question in a threat assessment inquiry is whether a subject *poses* a threat, not whether the subject *made* a threat.**
 - Some who make threats do not pose a threat.
 - Some who pose a threat never make threats.
 - Threats should be taken seriously, but should not be a necessary threshold to initiate an inquiry.

Conducting a Threat Assessment:

Threat assessment and threat management are integrated processes. The ultimate objective is to prevent attacks, not just to “predict” them. Assessments should guide risk management strategies and risk management interventions should be continuously monitored, assessed, and revised as necessary based on outcomes.

- **Gather information from multiple sources.**
 - Subject (see below), collateral persons, materials, and records.
- **Subject information:**

The purpose of gathering background information on the subject is not to determine if he is the “type of person” to become a Lone Offender, but to provide content for understanding his recent pattern of behaviors and communications and what they might suggest about whether the subject is planning or preparing for an attack.

- Identifying Information
- Background
- Current life information
- Relationships
 - Rejection by others
- Past times of extreme stress
- Interest in extremist/militant ideas, groups, or ideologies
- Mental status

- In prior studies of targeted violence, mental illness has not been a prominent causal factor. We do not know whether this same finding will apply to the preponderance of Lone Offender cases. In any case, it is probably more useful in assessing a subject's mental status to focus on whether he is sufficiently *organized* to carry out a complex act of targeted violence, rather than whether he has a mental disorder.
- Problems with severe depression, suicidal thoughts, or a lack of adequate coping mechanisms for a current emotional crisis may be even more important to assess than symptoms of psychosis or loss of contact with reality.

▪ **Recent Events & Reactions:**

- Violence sometimes occurs after an individual's coping system breaks down, creating a perceived sense of crisis and urgency to act. For some this precipitates a downward spiral.
 - The plan of attack can provide a sense of purpose or structure.
- Check for recent losses – people and loss of status/humiliation.
- Changes in functioning:
 - Self care
 - Despair
 - Hopelessness
 - Lacking self control
 - Feeling threatened
 - A significant, abrupt, self-directed life change, in appearance, spending habits, preparation of a will, and/or donation of personal belongings.
- Note behaviors of concern.

▪ **Pathway to Violence:**

- It is sometimes useful for an investigator to pose the threat assessment question as an appraisal of whether the evidence seems to indicate the subject is on a path toward a violent attack, and, if so, how fast he is moving toward attack and where intervention may be possible.
- Though sometimes professionals think of a pathway to violence as a steady escalation or progression, that will not necessarily be the case. There may be bursts of acceleration and deceleration or latent periods in which attack plans are not active or prominent. Movement along a pathway to violence is often driven more by situations, events, and how the subject perceives and reacts to them than by traits of the subject him/herself.

- Several factors that might be considered include the following:
 - **A – Attitudes that support violence**
 - Beliefs that violence is justifiable or even necessary under the current circumstances.
 - **C – Capacity**
 - Understanding the nature and extent of subject's capacity – material, skill, and cognitive organization – for an attack. This might include consideration of access to potential targets, opportunity, resources, and methods.
 - **T - Thresholds crossed**
 - Exploring attack-related behaviors to determine what steps, if any, the subject has taken toward action, including whether laws/rules have been broken and whether the subject has communicated his ideas to others.
 - **I – Intent**
 - A person may have ideas (or ideation) about an attack, without intending to act. Assessing the nature and degree of intent is an important feature of appraising the threat. An investigator might explore the subject's degree of commitment to action, exclusion of alternatives, and the extent of his planning.
 - **O– Others' Reactions**
 - Before an attack occurs, the Lone Offender may engage in behavior or communication that lead other people to be reasonably concerned. The subject may not make any direct threats, but his writings, drawings, online activities, and or “ominous statements” may be troubling to others.
 - **N– Noncompliance with Risk Reduction**
 - An investigator might consider the subject's ambivalence toward violence and whether he is at all motivated to prevent or avoid a violent act, whether he believes some kind of treatment or services might be effective, and what his history suggests about the likelihood that he will comply with conditions of supervision or a risk management plan. If a subject appreciates that he may be at risk of harming someone and is motivated to take action to avoid that outcome, his movement on a path toward violence might be more easily slowed or redirected.

Subject Interview:

Decisions about whether, when, and under what circumstances to approach or interview the subject directly must be made on a case-by-case basis. The BAU has assessed several situations in which directly approaching a suspect presented a risk of being provocative, potentially increasing his anger or paranoia, and heightening his sense of desperation or urgency to act.

There is no “one size fits all” approach, but approaches should be carefully planned and not driven by expediency or a desire to merely “check the box” of making contact with a particular subject. The BAU recommends that emphasis be placed on factors such as thorough preparation, selection of an interviewer, and the setting most likely to elicit meaningful information. Ultimately, it is crucial that investigators craft a thoughtful and strategic approach to the potential offender and avoid haphazard interviews and/or admonishments. These subjects are often hyper-sensitive to perceived slights and insults, and can easily misinterpret what we consider to be a legitimate law enforcement inquiry as a personal attack.

Threat assessment interviews should be thoughtfully approached and strategically crafted to the requirements of the specific situation and subject. As part of the threat assessment process, rather than immediately honing on the subject's ideology and conduct that aroused suspicion, the interviewer might instead focus initially on questions related to personal crises, financial stressors, relationships, goals and aspirations, role models, employment prospects, depression/despair, thoughts of suicide, and fears. This may not only be beneficial in rapport-building, but might also elicit information that will be critical in the threat analysis.

In the same way that threat assessment and management are integrated processes, the subject interview can be an intervention as well as an information-gathering device. Although specific interview/approach strategies should be developed on case-by-case basis, typically, a heavy-handed interview approach by law enforcement emphasizing threats and admonitions is not optimally effective and can be perceived as provocative.

An interviewer might consider designing an approach strategy to deescalate the subject and also to facilitate re-direction. An overarching goal of such an approach might be to gently amplify the subject's ambivalence. When a subject is considering or planning an attack, he often has some ambivalent or mixed feelings. Those feelings create some inertia in the subject's forward motion on a pathway to violence. The interviewer may be able to use that as part of a prevention-oriented approach.

A prevention-oriented interview approach is less like a lecture and more like a guided inquiry through the subject's motivation and reasoning. The interviewer usually talks less and does more listening and facilitation. While gathering information, the interviewer might pose questions around certain motivational themes, including the following:

- Drawbacks of Current Behavior:
 - What concerns do you have about what you're currently doing?
 - What concerns do others have about what you're currently doing?
 - What has this approach cost you?

- Benefits of Change:
 - If you did something different, how might that make things better for you?
 - How might doing things differently benefit (your family, cause, or people that matter to the subject)?

Putting Together the Pieces: Ten Key Investigative Questions

In arriving at a decision about whether a subject poses a threat, thoughtful consideration should be given to answering the following 10 key questions:⁸

#1. What motivated the subject to make the statements, or take the action, that caused him/her to come to attention?

- Basic “why” question - explore possibilities.
- Consider the credibility of informant and veracity of facts.
- Was it to get help, cause problems, avenge a wrong, commit suicide, or bring attention to a problem?
- Was it a means to an end – and is there a legitimization of the means?
- Motives for attack are usually related to target selection:
 - Not always motivated by animosity toward target.
 - Multiple targets may be considered.
 - Directions of interest may shift over time.
 - Why have some targets been ruled out?

#2. What has the subject communicated to anyone concerning his/her intentions?

- A direct threat is neither necessary nor sufficient.
- Many keep diaries or communicate to others.
- Question collaterals about unusual ideas or deterioration.

#3. Has the subject shown an interest in targeted violence, perpetrators of targeted violence, weapons, extremist groups or murder?

- It is important to explore a subject's interest in and pursuit of extremist/militant groups and ideas, not just whether he is a “member” of such a group. In the ECSP, most attackers had known interests in militant/radical ideas and groups, but were not active members. Many more potential attackers are influenced by extremist ideas than are “members” of any particular group or movement.
- May talk excessively about targeted violence.
- May inquire about the consequences of actions.

⁸ Fein, R. A., & Vossekuil, B. (1998). Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials. Washington, DC: United States Department of Justice.

- May make inquiries about acquisition of weapons.
- May contact prior perpetrators.

#4. Has the subject engaged in attack-related behavior, including any menacing, harassing, and/or stalking-type behavior?

- If harassment in the past, how was it stopped or resolved?
- Consider willingness to use violence, blaming target, unusual interest, planning or preparatory behaviors.
 - Location, weapon, subverting security
- Behaviors of concern:
 - Interest in extremism, evidence of ideas or plans to attack; communication or inappropriate interest or plan; following or approaching.
 - Any behaviors committed with a weapon or breaches of security are cause for concern.

#5. Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, etc. with indications that the subject has acted on those beliefs?

- Mental illness per se does not have a strong association with violence.
 - Substance abuse and psychotic symptoms make the most difference.
- Command hallucinations:
 - Hearing voices directing the person to do something
 - Compliance rates 40-89%
 - Factors associated with compliance
 - Familiar voice; Associated Delusion
- Delusions:
 - False, fixed beliefs that persist despite irrefutable evidence to the contrary
 - 60-77% may act on a delusion
 - Persecutory most likely
 - Inpatient study showed 40% had at least 1 violent event likely motivated by a delusion

#6. How organized is the subject? Is he/she capable of developing and carrying out a plan?

- Use a functional approach.
- Determine what step would be necessary to plan and execute.
- If mentally ill, assess subject's capacity when treated and untreated.

#7. Has the subject experienced a recent loss and or loss of status, and has this led to feelings of desperation and despair?

- Perceptions of life as unbearably stressful
- Losses: material, relational, status

- Family, intimate, occupational, self-image
- Hopelessness and suicide potential
- Inquiry into stressful events

#8. Corroboration – What is the subject saying and is it consistent with his/her actions?

- Attempt to corroborate as much information as possible.
- Compare the subject's account of ideas, motives and behavior to others' reports.
- Consider others' views on capacity for attack.

#9. Is there concern among those that know the subject that he/she might take action based on inappropriate ideas?

- If others are afraid of the subject, what is the basis?

#10. What factors in the subject's life and/or environment might increase/decrease the likelihood of the subject attempting to attack a target?

- Ascertain current and foreseeable circumstances that might stabilize or destabilize the individual.
- Support, supervision, or therapeutic alliance may be protective factors.

Threat Management:

An investigative assessment of the *likelihood* of an attack is not focused on some numerical probability estimate. Rather, the investigator must determine, based on the available facts, where there is a reasonable basis for concern about potential violence. Once that concern is identified, investigative activity often shifts to focus on how to mitigate/manage the risk or to prevent the attack from occurring. This is precisely why threat assessment and management should be viewed as integrated functions.

Historically, law enforcement agencies have not specialized in developing or implementing long-term threat management strategies. When a reasonable concern is identified, the nature and degree of risk must be monitored and follow-up action should ensue. This is especially relevant for potential Lone Offender situations, where a subject has exhibited behaviors of concern, yet criminal activity is insufficient to justify an arrest or resource-intensive technical coverage. Because of the nature of these cases and law enforcement resource limitations, continuous physical surveillance is usually not feasible.

The BAU strongly recommends that investigators consider prevention to be the primary objective of threat management. A variety of strategies and tools may be available at different stages of the investigation. Traditional threat management strategies include incapacitation (through arrest or detention), target hardening (where the intended target is specifically identified or identifiable), and intensified subject supervision. A subject might also be monitored more closely through third parties or investigative sources. In some circumstances, it might be possible to de-escalate or address the subject's underlying grievance. For example, if a subject has escalated on the pathway to violence as the result of a dispute with a government organization, an investigative team might explore whether an ombudsperson or mediator might be available to intervene. Actions like this may serve to diffuse, rather than intensify, a subject's anger and movement on a pathway to violence.

Effective threat management plans often require some degree of coordination across different systems, not just a single point of law enforcement contact. In circumstances where a significant mental health concern has been acknowledged or identified, some degree of collaboration with mental health specialists might be possible.

Most threat management plans will involve some consideration of the following:

- *Determine whether there is a need for immediate containment.* If a subject poses an imminent risk for a violent attack, the investigator should consider containment options. This may include detention, arrest, or hospitalization. The main objective is just to ensure immediate safety and to buy time while diminishing the intensity of the subject's commitment to attack.
- *Determine whether target hardening measures are necessary.* If the investigator believes that there is a proximate risk to an identified or identifiable target (e.g., a specific named person), the necessity and appropriateness of various protective measures should be considered to reduce the target's vulnerability.

- *Identify mitigators.* Based on the subject's grievance, motivation, or other dynamics driving a potential attack, the investigator might identify available resources or services that might redirect him or reduce his risk. Medical, mental health, social service, interpersonal support, criminal justice, or victim service resources might all be considered.
- *Mobilize and coordinate resources.* If immediate incapacitation is not indicated, after mitigators are identified, the investigator should facilitate or coordinate the process of linking the subject to the proper people or agencies to provide those services (or the necessary monitoring/supervision). Often a simple referral or handing him a phone number will not be sufficient to ensure that the connection is made. The objective here is to engage the subject in a risk management plan and to take concrete steps to mobilize that plan.
- *Monitor and follow up.* Even the best risk management plans can falter over details. With needs and resources identified and mobilized, the investigator might think through the action steps of implementing the threat management plan. Who has responsibility for each element? How and when will the activities be done and monitored? It is usually advisable to have objective markers of redirection or of reduced risk, to include some way of concretely determining whether the plan is or is not working and whether, when, and the extent to which the subject's attack risk has been mitigated.

Conclusion

The BAU continues to collaborate with established threat analysis experts in government, academia and the private sector. The FBI's ongoing Lone Offender study – as one product of that collaboration - is designed to inform operational assessments. As the study progresses, BAU will provide a series of brief, interim reports to CTD, field offices, and JTTFs based on preliminary findings as they become available. As a next step, the study team is preparing a document describing the study's key operationally-driven questions. We will reach out to our field partners, and welcome their suggestions, to assure that the study is optimally responsive to operational and investigative needs. The BAU is also working actively to enhance its operational database of targeted violence incidents and offenders to provide law enforcement officers access to knowledge about observable, pre-incident indicators of planned attacks. We hope that this kind of knowledge will further refine the FBI's assessment of fringe subjects and other potential attackers, thereby enhancing our effectiveness and bolstering our homeland security. The BAU continues to be available as a resource for behavioral-operational assessments and for interview and threat management strategies tailored for individual subjects, in critical threat scenarios.