



# THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION  
AND  
HOMELAND SECURITY

MARCH 2013  
ACTIVE SHOOTER

VOLUME 11 NUMBER 9

Facility Upgrades.....	2
Shooter-in-Waiting.....	4
Issues in CI/KR.....	7
TISP Symposium.....	9
Mental Illness.....	10
IEEE/IFIP Conference.....	11
Prevention & Detection.....	12
Attacks on Gov't Facilities.....	15
Fatigue Risk Symposium.....	21

## EDITORIAL STAFF

**EDITOR**  
Kendal Smith

## JMU COORDINATORS

Ben Delp  
Ken Newbold

**PUBLISHER**  
Melanie Gutmann

Click [here](#) to subscribe. Visit us online for this and other issues at <http://cip.gmu.edu>

Follow us on Twitter [here](#)  
Like us on Facebook [here](#)

In this month's issue of *The CIP Report* we focus on the Active Shooter, a problem that has weighed heavily on the American populace in recent months. With the Sandy Hook and Aurora tragedies still fresh in everyone's minds, we have included articles from the military, law enforcement, academia, medical profession, and private industry in hopes of shedding light on this difficult issue.

First, Major Chuck Ergenbright outlines an approach for mitigating the effects of Active Shooter incidents in high occupancy facilities, centered on a Victim Initiated Mitigation system and standardized law enforcement training and vulnerability evaluation.

Second, Dr. Mark Coulsen examines the Active Shooter-in-Waiting, dispelling myths and advocating an integrative approach. Maryland University Police Captain Robert Mueck then discusses Active Shooter issues for critical infrastructure and key resources, particularly regarding schools and insider threats. Psychiatrist Frank Ochberg then evaluates Active Shooter incidents in light of mental illness. Next, MBA candidate Lambert Ninteman argues for the use of new technologies such as head-mounted display systems to assist in detection and prevention efforts. Finally, Battelle's Ed Jopeck, Aaron Alford, and Kelly Shaffer provide an accounting of attacks on government facilities by the mentally ill, offering strategies for prevention and defense.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.



School of Law  
CRITICAL INFRASTRUCTURE  
PROTECTION PROGRAM

Mick Kicklighter  
Director, CIP/HS  
George Mason University, School of Law

## Defeating the Active Shooter: Applying Facility Upgrades in Order to Mitigate the Effects of Active Shooters in High Occupancy Facilities “A Meaningful Change”

by Chuck Ergenbright

In response to the tragedy that unfolded in Newtown, CT our President has called for a “meaningful change.” After conducting an extensive case study review and analysis of U.S. Active Shooter incidents as part of a Master’s Thesis completed at the Naval Postgraduate School,<sup>1</sup> the lack of victim initiated means for mitigating the Active Shooter threat in Institutions of Higher Education (IHEs) and High Occupancy Facilities (HOFs) became apparent as the most important variable and focused the recommendations. While the research scope for the thesis was IHEs, the resulting recommendations are exportable to all HOFs to include primary schools such as Sandy Hook Elementary. The average duration of Active Shooter incidents in U.S. IHEs is 12.5 minutes. In contrast, the average response time of campus and local law enforcement to these incidents is 18 minutes. In the majority of Active Shooter incidents affecting U.S. IHEs, the emergency response time greatly exceeds the incident duration and affords law enforcement authorities no opportunity to interdict the shooter or prevent further casualties. This stark contrast between response require-

ments and response capability produces a considerable delta of dead, injured, or potential victims. The intent of the recommendations included in the thesis is to reduce the Rate of Kill of Active Shooters in U.S. IHEs. The research includes 14 case studies examining lethal Active Shooter incidents occurring in U.S. IHEs, as well as the Oslo and Utoya Island Active Shooter event which occurred in Norway. Data analysis on each of these incidents revealed facility composition as a critical vulnerability common to all of these incidents. Accordingly, the recommendations suggest a practical implementation of facility upgrades capable of mitigating the deadly effects of Active Shooters.

Although every Active Shooter event is a tragedy, the raw emotions recently uncovered by the Sandy Hook Elementary shooting resonated in the hearts of all American’s and truly defines the core of what this country regards as its most precious treasure; our children. Although this is a complex problem, our country has been here before. However, this solution will require a paradigm shift, leadership, and resolve. President Truman

faced a similar dilemma during his presidency. The U.S. Department of Homeland Security and the U.S. Fire Administration National Fire Data Center created a joint publication entitled School Fires which states that the United States experienced 10,000 fire related deaths annually in IHEs and HOFs during his presidency. In similar fashion to the Sandy Hook tragedy of 2012, one such disaster, a 1958 fire which consumed Our Lady of the Angels grade school on the West Side of Chicago, killing 92 children and three nuns, provided the catalyst for change regarding fire prevention.<sup>2</sup> In response to this complex problem, President Truman convened the President’s Conference on Fire Prevention where victim initiated response measures were identified as critical components to an effective threat mitigation plan. As a result, the current fire code we are familiar with today was developed and school fire casualties were reduced to zero after 1958. In fact, to this very day, no child has died in a school fire since 1958. This council determined that by placing a tool in the hands of potential victims and providing a standardized response, the fire threat could be effectively

*(Continued on Page 3)*

<sup>1</sup> Charles E. Ergenbright and Sean K. Hubbard, *Defeating the Active Shooter: Applying Facility Upgrades in Order to Mitigate the Effects of Active Shooters in High Occupancy Facilities*, Naval Postgraduate School, June 2012, <https://www.hsdll.org/?view&did=718911>.

<sup>2</sup> Rex Huppke, “Our Lady of the Angels: The Fire That Changed Everything,” Chicago Tribune, *Chicagoland*, November 29, 2008, <http://www.chicagotribune.com/news/local/chi-our-lady-of-the-angels-fire-students-killed,0,6650568.story>.

(Continued from Page 2)

mitigated. Although this vignette provides a great example of our country solving a similar complex problem, there is currently no such solution for the Active Shooter threat. Meanwhile, 35 students are murdered and a quarter of a million more are seriously injured in acts of school violence annually.<sup>3</sup>

After extensive research, we derived four immutable Active Shooter realities that must be addressed. First, these acts of extreme violence cannot be prevented. Second, there will always be a delay between initiation of violence and Law Enforcement response. Third, in the time separating the first and last shots fired, the only individuals who have the capacity to react are potential victims. Finally, within current U.S. security configurations, the only individual predominantly in control during an Active Shooter incident is the shooter himself. In order to counter these realities, we recommend a holistic approach to Active Shooter mitigation including prevention/preemption efforts, mental health screening/treatment, law enforcement response, and victim actions. However, the most critical component and first step of this plan must be a Victim Initiated Mitigation (VIM) system incorporating automated control measures and complementary response protocols. Our prioritized recommendations include:

First, secure our schools and

HOFs with a Victim Initiated Mitigation (VIM) system. A properly networked VIM system can immediately notify law enforcement while simultaneously containing the threat utilizing facility lockdown and mass alert protocols. Second, standardized training for potential victim response emphasizing Avoid, Deny, and Defend (A.D.D.) methodology must be incorporated in schools nationwide. Third, law enforcement training must be standardized to encourage first responder initiative and direct-to-threat methodology required to neutralize threats in a timely manner. Fourth, prevention/preemption and mental health screening efforts must facilitate a culture of safety and identify threats before they materialize. Finally, a national threat mitigation standard that evaluates schools based on vulnerability to Active Shooter threats compared to a standard such as the proposed Standard Operations for Automated Response (S.O.A.R) which evaluates prevention/preemption measures, law enforcement readiness, and Victim Initiated Mitigation system implementation must be prescribed.

Our recommendations are in keeping with guidance issued by the National Clearinghouse for Educational Facilities for Crime Prevention through Environmental Design regarding access control measures and adhere to directives issued by the National Incident Management System regarding preparedness, interoperability, standardization of communications and capabilities of Incident Command Centers, as well as emergency response protocols.



Additionally, these recommendations attend to preparedness questions raised by DHS. Attention given to these considerations has produced a proposed system that offers a flexible core mechanism for a coordinated and collaborative incident management incorporating common terminology while facilitating an integrated response. We feel that these recommendations, if implemented, could have the same notable impact to Active Shooter mitigation as implementation of the current fire code has had on preventing fire related casualties. Although the proposed facility upgrades are expensive, project funding suggestions included in this research resulted in large universities being able to fully recoup their initial investment in less than seven years and benefit from residual income thereafter. Similar financial solutions are available on a national scale for public schools and other HOFs and should be pursued in order to protect our most valuable investment; our children. ❖

<sup>3</sup> Dave Grossman, "School Shooting Contingency Plans & Considerations," *Killology Research Group: A Warrior Science Research Group Partner*, 2000, [http://www.killology.com/school\\_notes\\_plans.htm](http://www.killology.com/school_notes_plans.htm).

\*Image courtesy of Phiseksit/FreeDigitalPhotos.net

## Prevention Rather Than 'Cure': Identifying the Active Shooter-in-Waiting

by Mark Coulson, Ph.D.,  
Reader in Psychology, Middlesex University, London UK

When faced with traumatic events, we are motivated to create narratives, and tell stories about why things happened the way they did. This helps us gain some feeling of understanding of people and events, and how we can absorb the events into our views of how the world works. In an Active Shooter incident we become poignantly aware of the narratives presented to us concerning those who lost their lives, those who lost loved ones, and the short and long term effects on the communities where such events transpired. We then naturally turn to details of the life of the perpetrator with a similar desire to understand why they did what they did, to minutely examine their backgrounds both recent and more distant, their hobbies and interests, their relationships with others, and their own psyches. We are assisted in this endeavor by the media, who focus on anything and everything as potential sources of illumination for some of the darkest corners of the human mind.

While the desire to understand is human nature, we are fallible individuals operating under cognitive limitations, and are ill-equipped to reason and draw conclusions from the mass of data

which may contribute to the tragic transformation a person undergoes in becoming an Active Shooter. A wealth of experimental research has demonstrated that, when forming judgments about other people, we place undue emphasis on their idiosyncratic characteristics, especially if these offer immediate and satisfying 'explanations' for their behavior. For example, if we are told that 'Angus is a loner who collects guns and knives and likes to watch war movies' and then asked 'Is Angus more likely to be a psychopath or a librarian?' we tend to focus on specific details to the exclusion of base rate data (that there are many more librarians than psychopaths, and consequently far greater numbers of people with this particular set of interests will be librarians as opposed to psychopaths). This focus on the particular and the specific tends to persist even when data are made available. In short, people are generally poor at interpreting data and using them to draw accurate conclusions.<sup>1</sup>

Active Shooter incidents are extremely rare, and extremely difficult to generalize from. In a recent FBI review, 154 cases between 2002 and 2012 were

identified, representing a tiny fraction of one percent of the U.S. population.<sup>2</sup> Any seemingly distinctive or unusual interests, behaviors or psychological characteristics of Active Shooters are likely to be so numerous in the general population that their predictive accuracy is extremely low. The relatively small number of Active Shooter incidents makes extrapolating general patterns of pre-incident behavior or 'warning signs' extremely problematic. As a consequence, official advice on identifying Active Shooters-in-Waiting (ASIW's) is well intentioned, but is necessarily limited to easily observed characteristics or events such as what has recently happened at work or school, changes in demeanor or behavior, and so on. Indeed, such is the variety of behavioral changes which has been observed to (actually or potentially) occur in Active Shooters, that advice may be contradictory (for instance, key indicators may include being aggressive towards others or being bullied, paying more or less attention to security staff and access/egress to facilities). Pre-incident behavior may, as outlined

*(Continued on Page 5)*

<sup>1</sup> Gerd Gigerenzer, *Reckoning with Risk: Learning to Live with Uncertainty*. Penguin Books: London. (2002).

<sup>2</sup> DHS-FBI Bulletin: "Recent Active Shooter Incidents Highlight Need for Continued Vigilance," (December 27, 2012) Available at <http://publicintelligence.net/dhs-fbi-bulletin-recent-active-shooters/>.

(Continued from Page 4)

above, be of little diagnostic value in that a large proportion of not-at-risk people may be misclassified as ASIWs (for instance, failed love relationships, an observation potentially applicable to vast swathes of the population, and almost ubiquitous among some demographic groups such as teens). Finally, advised warning signs may be essentially unrelated to violent behavior (for instance, participation in violent video games).<sup>3</sup> There are also historical assumptions about pre-incident behavior, now largely discredited, such as the 'forensic triad', elements of which still appear on lists of behaviors to look out for when assessing Active Shooter risks.

While an Active Shooter event most probably involves a triggering event or sequence of events, such events in isolation are insufficient, instead representing the final parts of a complex biopsychosocial interaction of genetic predispositions, psychological characteristics and experiences, and environmental contingencies which result in the ASIW. Downturns in fortune, personal or professional losses, or failed relationships (as opposed to global, national or regional change: Active Shooter incidents are almost always personal rather than political), are parts of the complex but are insufficient as explanations.

What then might be done to identify an ASIW? Converging

themes from a variety of sources suggest that an inter-disciplinary approach focused on prediction and consequent screening may offer some hope. First, contemporary models of personality suggest there may be 'vulnerable' personality types. Such personalities fall well within the normal range, meaning the personality is not in itself causal, but the particular combination of characteristics renders the individual more susceptible to certain behavioral patterns such as violence. The dominant 'Big-5' model, which sees personality as consisting of five characteristics (Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism) possessed by all people to different degrees, presents a myriad of personality types, as the degree to which one possesses each characteristic is entirely independent of the others. Some recent analyses have suggested that certain combinations of these characteristics (crucially, high Neuroticism combined with low Agreeableness and low Conscientiousness, a personality which might be described as temperamental, distant, and careless/non-confirming) may predispose people to respond aggressively to violent video game play, however it is important to recognize that such analyses should not be overextended.<sup>4</sup> There are insufficient data to permit the same sorts of predictions to be made about ASIWs, and more research is clearly required, but personality almost certainly represents an

important risk factor.

Second, reviews of other psychological and experiential risk factors have begun to more clearly identify commonalities across Active Shooters, and also identify those which, while appealing in the narratives created by the media and other social and political commentators, are in all likelihood not part of the ASIW complex. Key indicators include a history of mental illness (whether diagnosed or not), and in particular suicidal attempts or ideation. The ASIW's perceptions of themselves as bullied or persecuted are more predictive than whether they are in fact bullied or persecuted.<sup>5</sup> These perceptions, often referred to as cognitive or attributional style, have profound implications for self-generated understanding of the world and the behaviors which this influences. Whereas one person might see no threat to status or safety in a particular situation, another may feel profoundly threatened, and consequently more likely to act aggressively in self-preservation. How people make sense of the world varies along multiple dimensions, perhaps the most relevant to the ASIW being the degree to which we see our fortunes as depending on our own actions or those of the external environment. Belief in the latter, labeled an *external locus of control* has been

(Continued on Page 6)

<sup>3</sup> Chris Ferguson, Mark Coulson & Jane Barnett, "Psychological Profiles of School Shooters: Positive Directions and One Big Wrong Turn," *Journal of Police Crisis Negotiations*, 11 (1) 1-17 (2011).

<sup>4</sup> Patrick M. Markey & Charlotte N. Markey, "Vulnerability to Violent Video Games: A Review and Integration of Personality Research," *Review of General Psychology*, 14 (2) 82-91 (2010).

<sup>5</sup> *Supra*, note 3.

(Continued from Page 5)

linked with aggressive behavior,<sup>6</sup> a finding which is of serious concern given that belief in external loci of control appears to be increasing in young Americans.<sup>7</sup>

Third, the field of behavioral genetics has begun mapping some of the complex biosocial interactions between genetic predispositions and environmental factors. It appears, for instance, that neither genetic predisposition (defined as possession of particular alleles of specific genes) nor childhood mistreatment are predictive of violent antisocial behavior, but that a combination of the two elevates risk.<sup>8</sup> Although these findings are potentially important, it should be noted that they are far from well established, and at present offer no great utility

as screening tools.

Policy, strategy, and advice at all levels of infrastructure are required for dealing with the sudden, unpredictable, and catastrophic effects of an Active Shooter event. Identifying the ASIW, however, demands new approaches to research and the integration of evidence across disciplines in order to generate usefully predictive models.<sup>9</sup> Such models need to consider the inclusion or exclusion of variables in light of research evidence rather than after-the-fact observations, and comforting but misleading narratives. In particular, previous episodes of mental illness (whether diagnosed or not), suicide attempts or suicidal ideation, vulnerable personality types, downturns in personal circumstances, and a cognitive style

which tends towards persecutory and external attributions, appear to constitute the key elements of any model. Although current models designed to predict violence show only moderate levels of accuracy,<sup>10</sup> and the importance and variety of genetic factors remains largely unknown, there is reason to be optimistic that formal tools which evaluate the risk of an ASIW transforming into an Active Shooter may be within reach. Using such tools as early warning signs, leading (eventually) to genetic screening for the presence of critical alleles which jointly raise alarms, could lead to greater emphasis on a strategy of prediction and prevention, and a corresponding reduction in the terrible costs of Active Shooter events. ❖



<sup>6</sup> Marion T. Wallace, Christopher T. Barry, Virgil Zeigler-Hill & Bradley A. Green, "Locus of Control as a Contributing Factor in the Relation Between Self-Perception and Adolescent Aggression," *Aggressive Behavior*, 38 (3) 213-221 (May/June 2012).

<sup>7</sup> Jean M. Twenge, Liqing Zhang & Charles Im, "It's Beyond My Control: A Cross-Temporal Meta-Analysis of Increasing Externality in Locus of Control," 1960-2002. *Personality and Social Psychology Review*, 8 (3) 308-319 (2004).

<sup>8</sup> Avshalom Caspi, Joseph McClay, Terrie E. Moffit, Jonathan Mill, Judy Martin, Ian W. Craig, Alan Taylor & Richie Poulton, "Role of Genotype in the Cycle of Violence in Maltreated Children," *Science* 297, 851-854 (2 August 2002).

<sup>9</sup> John M. Harris Jr. & Robin B. Harris, "Rampage Violence Requires a New Type of Research," *American Journal of Public Health*, 102 (6) 1054-1057 (June 2012).

<sup>10</sup> Mary Ann Campbell, Sheila French & Paul Gendreau, "The Prediction of Violence in Adult Offenders: A Meta-analytic Comparison of Instruments and Methods of Assessment," *Criminal Justice and Behaviour*, 36 (6) 567-590 (June 2009).

\*Image courtesy of YaiSirichai/ FreeDigitalPhotos.net

## Active Shooter Issues in CI/KR

by CPT Robert P. Mueck, Training Academy Director, University of Maryland Police

The United States, as a Nation, is experiencing something that is altogether frightening and terrible in the form of mass shootings. This issue requires introspection from all sides, yet we stand as divided as our political parties. Clearly there is no easy answer. In the last 20 years, we have experienced mass shootings in the work place, colleges, churches, movie theaters, malls, restaurants, military bases, and schools. Among 63 identified mass shootings from 1980 to 2012, 12 occurred at schools, 19 occurred in the workplace and 32 occurred at other sites.<sup>1</sup>

Mass shootings of all types draw media attention, but school shootings seem to be particularly newsworthy. According to the Centers for Disease Control and Prevention (CDC), from 1992 to 2006, less than 1% of all homicides involving children ages 5-18 occurred at school. Yet this data does not account for the number of planned school shooting attacks that have been prevented. According to National School Safety and Security Services there have been 120 prevented attacks between 2000 and 2010.<sup>2</sup>

I have heard arguments that schools should be identified as a Critical In-



frastructure that require protection. While we have identified vulnerability in the security of our schools, the more appropriate designation for schools may be as a Key Resource. No matter what we decide, it is clear that we believe in the value of life, above all our children.

### Active Shooter as the Insider Threat

There is no profile we can use to identify Active Shooters. They cross all ranges of gender, race, age, and economic status. We used to refer to this as “going postal,” a term derived from a time when the U.S. Postal Service suffered from a series of workplace shootings in the 1980’s. In their case, it was a series of acts by disgruntled employees that brought the violence to the workplace. This is no different than other Active Shooters who feel a need for

revenge for perceived injustices, whether at work or in school. Tragically, one can be “wronged” in one arena but commit the attack in another, such as the Newtown, Connecticut shootings in December 2012.

In most cases, the Active Shooter is the ultimate insider threat. The disgruntled employee, the student with feelings of persecution, the faculty member who is refused tenure; they are all insiders. These are people have access to facilities based on their membership in that environment. When they attack, they exploit their access and use it to target their victims. This is difficult as we try to ascertain if the person is just odd, or is going to become violent. We see differences with shootings like the ones at various malls

*(Continued on Page 8)*

<sup>1</sup> Josh Filler, “Are Schools Critical Infrastructure in Need of Protection from Active Shooters?” *Emergency Management*, December 21, 2012, <http://www.emergencymgmt.com/emergency-blogs/homeland>.

<sup>2</sup> See <http://www.schoolsecurity.org/>, retrieved 01/19/2013.

(Continued from Page 7)

or churches. The shootings at the movie theatre in Aurora, Colorado and Newtown, Connecticut are different, as the shooters were not part of the environment. They were not insiders, and yet managed to wreak havoc with their attacks. Similar to terrorism, this is a mutating threat that is a challenge to government at all levels.

After the tragedy at Virginia Tech, college campuses around the country have developed multi-disciplinary threat assessment teams to identify “students of concern” and engage them before they resort to violence. The size of the team can vary, but minimally includes campus police, counseling centers, student conduct, student affairs, and others with a vested interest. This is similar to the private sector where corporations conduct threat assessments of employees exhibiting behavior of concern.

In 2002, the U.S. Secret Service and U.S. Department of Education published the “Safe Schools” study. They advocate the adoption of threat assessment programs by schools, which is effective for the insider. Threat assessment teams are very effective in the individual violence process, and the study identified ten findings that have implications for the use of threat assessment protocols.<sup>3</sup>

*Key Finding 1:* Incidents of targeted violence at school rarely are sudden, impulsive acts.

*Key Finding 2:* Prior to most inci-

dents, other people knew about the attacker’s idea and/or plan to attack.

*Key Finding 3:* Most attackers did not threaten their targets prior to advancing the attack.

*Key Finding 4:* This is no accurate or useful “profile” of students who engage in targeted school violence.

*Key Finding 5:* Most attackers engaged in some behavior, prior to the incident, that caused others concern or indicated a need for help.

*Key Finding 6:* Most attackers had difficulty coping with significant losses or personal failures. Many had considered attempted suicide.

*Key Finding 7:* Many attackers felt bullied, persecuted, or injured by others prior to the attack.

*Key Finding 8:* Most attackers had access to and had used weapons prior to the attack.

*Key Finding 9:* In many cases, other students were involved in the attack in some capacity.

*Key Finding 10:* Despite prompt law enforcement responses, most attacks were stopped by means other than law enforcement intervention and most were brief in duration.

### **The Mutating Threat**

Law enforcement has adopted their response to these kinds of incidents.

Each incident brings with it lessons learned, and adjustments were made after each. Like other professions, these issues are discussed at local, regional, and national levels. For instance, the University of Texas shootings in 1966 lead to creation of SWAT teams. LAPD was the first to identify a way to counter an attack similar to what happened at UT Austin, and many departments around the country followed suit. Over the years, organizations such as the National Tactical Officers Association (NTOA), International Association of Chiefs of Police (IACP), and U.S. Department of Justice (DOJ) have studied such attacks and adjusted tactics to counter them.

Columbine changed tactics on a national scale. No longer do officers wait for SWAT to show up. Various tactics are used to counter the Active Shooter threat, but in the end, they are all similar. Law Enforcement is better armed and trained to stop the shooting. Where a decade ago very few law enforcement agencies had patrol rifles, that is now the exception rather than the rule. The issue we now face is the response time for law enforcement. Shootings happen very quickly and frequently end when officers arrive with the shooter taking his own life.

### **A Physical Proposal**

In a paper from the Naval Post Graduate School, authors Charles Ergenbright and Sean Hubbard recommend applying principles

(Continued on Page 9)

<sup>3</sup> United States Secret Service and Department of Education, *Threat Assessment in School: A Guide to Managing Threatening Situations and to Creating Safe School Climates* (2002).

(Continued from Page 8)

of fire safety engineering to the issue.<sup>4</sup> They argue that upgrades to facilities can isolate people bent on violence in something called the Victim Initiated Response and Automated Lockdown (VIRAL). In modifying buildings along the lines of fire engineering, shooters could be isolated, thereby limiting their kill rate and minimizing their ability to create a high body count. This system could alert local law enforcement while only allowing egress from a building. An interesting concept, the issue here may be the cost of retrofitting each building and working out how it fits into existing fire codes. Still, it has its merits and deserves an honest look.

#### **Detecting a Move Toward Violence**

Someone who is escalating in violence and planning an attack uses steps similar to those used to commit a terrorist attack. They need to decide on their target and surveil it to look for weaknesses. They need to gather materials, purchase weapons and ammo, and plan their method of attack. As attackers go about doing all this, there are opportunities for people to observe their behaviors and report them to law enforcement. Times have changed, and where law enforcement might have dismissed this kind of behavior in the past, that is no longer the case.

Of particular note is the issue of “leakage.” This refers to the communication shooters make before their attack, where they allude to their ac-

tions. Particularly true of younger shooters, social media makes this a challenge to law enforcement. Threatening or disturbing messages can be taken out of context or are easily misunderstood. With no voice inflexion or context for the statements posted in social media, law enforcement and other officials have no choice but to follow up on such communication when posted.

Ferretting out what is fantasy, what is a joke, and what is real can be very difficult with high stake consequences.

As we enter this new era involving mass violence, we need to work together to find a solution. Everyone has a stake in this issue; only together can we address it. United we stand...divided we fall. ❖

## **Registration Now OPEN!**

### **THE 2013 CRITICAL INFRASTRUCTURE SYMPOSIUM**

**“Advancing Full Spectrum Resilience”  
April 15-16 • Thayer Hotel, West Point, New  
York**



Hosted By: The Infrastructure Security Partnership, Society of American Military Engineers, the U.S. Army Corps of Engineers Engineer Research and Development Center, and the U.S. Military Academy at West Point

**Please Click Here for Additional Information.**

<sup>4</sup> Charles E. Ergenbright and Sean K. Hubbard, *Defeating the Active Shooter: Applying Facility Upgrades in Order to Mitigate the Effects of Active Shooters in High Occupancy Facilities*, Naval Postgraduate School, June 2012, <https://www.hsdl.org/?view&did=718911>.

## Preventing Murder by the Seriously Mentally Ill\*

by Franch Ochberg, Md.\*\*

Is T. J. Lane, the seventeen year old boy who allegedly killed three classmates in Ohio, mentally ill? We do not know. But this tragedy evokes other recent spree shootings that have ignited a national conversation, sometimes harsh, but generally thoughtful—and urgent: What can prevent murder by someone who is spiraling into serious and deadly illness?

When a mentally ill person is a killer—a rare but terrifying phenomenon—it is hard to empathize. We think of him as alien. We have no basis for identification. We are shocked by the deed. Indeed, some killings are so bizarre as to evoke horror, disgust and disbelief.

Oddly enough, we may also be fascinated, even attracted to such cases. Why? Consider fairy tales, campfire stories, horror movies, certain bible stories, and the mantra in journalism, “If it bleeds it leads.” There is something in us that causes us to consume stories of madness and mayhem from early childhood, giving us reference points should the real thing happen when we are older. It is part of our culture and of our biology. Given our familiarity with fairy tale monsters, and our inability to identify with the witch, giant or ogre, it is no wonder that we are attracted to the story, but

repelled by the person who kills because of major mental illness.

The Tucson shootings, the Virginia Tech massacre and the attempted assassination of President Ronald Reagan—all clearly the result of major mental illness—were no fairy tale or horror film. We can and must get serious about understanding mentally ill killers—about intervening before the worst happens, caring for these individuals, and overcoming our sad history of neglect.

We can't go on letting our revulsion cloud our compassion. These people are suffering from brain disease. They are not intrinsically evil, but as we have seen in case after case, ordinary measures—whether conventional law enforcement, college policies or the existing mental-health system—are not adequate when it comes to identifying and containing the small number of mentally ill who are truly dangerous.

When the brain disease is schizophrenia, signs usually appear in recognizable form in late teens or early twenties. The person with the disease may or may not recognize it. In the beginning, there can be terror as a teen or young adult feels he is losing his mind. The fear of falling apart is relieved by the delusion

of being god-like and being pursued or polluted. Schizophrenic delusions are usually grandiose and persecutory. If the disease is caught before the delusion becomes fixed, the outcome is better. But even after a delusion is formed, treatment can help.

Only a fraction of persons with schizophrenia become dangerous. When they do, it usually is because their hallucinations command violent acts and because their delusions convince them they must kill for their own good or for the good of others. It is also because they have escaped from social contact and have gained access to lethal weapons.

As a matter of public policy, we have dismantled the state mental hospitals because they became abusive. But we have failed to fund the alternative, a supervised system of humane local services. We have abandoned the seriously mentally ill to their own devices, or to temporary lodging in jail. While the Ohio shooter has yet to undergo a psychiatric examination, there are many cases of mass killing where a history of illness and isolation is clear.

While we should do the whole job

*(Continued on Page 11)*

(Continued from page 10)

of caring for the seriously mentally ill, we must do the narrow job of caring for the dangerously mentally ill. We need to do more than expel them from school, military service or employment.

So what can be done? We can start by expanding court ordered civil commitment—outpatient and inpatient—to include the creation of a new cadre of professionals.

This cadre needs the skills of the Secret Service agent who knows how to befriend and follow those on the “watch list” of persons at large who have written bizarre letters to the President. They need the compassion of the nurse who considers care her calling. They need the guts and consistency of the resourceful parole officer who keeps his client away from temptation and out of prison.

Most of all, this new friend of the court must be able to detect when a person with a psychosis or a major depression has interest in using

deadly weapons. Laws preventing access mean little in gun-saturated America. A new professional, practical and resourceful, needs to be created and deployed to understand and intervene.

Outpatient civil commitment can work. It requires expert diagnosis and a fair judicial hearing to establish the need for confinement or monitored release. Then it requires a newly designed, well-managed system to assure that a person who passes the threshold for court commitment, but does not meet the requirement of hospital confinement, has a friend of the court who provides frequent contact, monitoring for possession of weapons and referral for medication and hospitalization when needed. This new “friend” or “monitor” will need training based on the experience of those who are comfortable, knowledgeable and effective in dealing with emerging schizophrenia and with similarly severe psychiatric conditions. Schizophrenia is not the only mental illness associated with

notorious killing. There are depressives who are so hopeless and so humiliated that they explode into homicidal and suicidal rage. There are brain-damaged people with injuries or tumors who suffer and seethe and explode. There are intoxicated people who lose all sense of reality and kill their imaginary demons. The new system and new agent may not be able to prevent every tragic episode. But we can begin where prevention can work. Instead of ridiculing or demonizing or abandoning those who are ill and deluded and dangerous, we can identify and connect and supervise and treat. ❖

*\*This article was originally published by CNN.com and can be found [here](#).*

*\*\*Dr. Frank Ochberg is Clinical Professor of Psychiatry at Michigan State University and former Associate Director of the National Institute of Mental Health.*



## The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks

Budapest, Hungary  
June 24, 2013



A resilient system is a system that can, in the face of unknown, large-scale events, recover from the failures and maintain its functions. It is known that many systems, such as biological systems, human mind, social systems, and dependable engineering systems exhibit this property. However, it is not clear how we should identify general “resilience” properties or strategies applicable to systems in many different domains. The purpose of this workshop is to bring the insights from various fields of resilient systems and explore common research challenges and design principles in the new discipline of “systems resilience.”

**Information and registration at: [HTTP://2013.DSN.ORG/](http://2013.DSN.ORG/)**

## Active Shooter Events: Detection & Prevention

Lambert Ninteman, MBA Candidate, San Diego State University  
Team Captain, San Diego State University, Qualcomm Tricorder X-Prize Team

*Agility and resilience. Engagement and integration. These are some of the key principles that will define Homeland Security 3.0.* (DHS Secretary Janet Napolitano, The Brookings Institute, February 26, 2013).

As the ten-year anniversary of the Department of Homeland Security approaches, a great deal of attention has been focused on successes and failures of that formative period. Five core missions have been defined for DHS: terrorism, border security, immigration enforcement, cybersecurity, and disaster preparedness and response. Not all threats, however, fit so neatly into that rubric; according to Secretary Napolitano, “we were also confronting the reality of homegrown threats, including from individuals who may have no particular connection to terrorism, but nevertheless can threaten our cities and communities, our schools, and our places of worship.”<sup>1</sup> Among those home-

grown threats is the ever-present danger of an Active Shooter event.

The Active Shooter booklet published by DHS defines an Active Shooter as, “an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly.”<sup>2</sup>

Like a lightning strike or drunken driving accident, the causes are often too easy to ascertain only after tragedy has struck. Being prepared for bad weather or alert driving can help to a degree, and is always considered best practice, but as events of these types are unforeseeable, it is only the result that is predictable.

There have been a number of recent high-profile Active Shooter

incidents over the past year, including Aurora and Sandy Hook, underscoring the need for the development of effective methods of detection and prevention of such events. A great deal of research has been undertaken in the past decade attempting to identify key behaviors and triggers associated with an Active Shooter event, whether targeting institutes of higher learning, or workplace environments.<sup>3</sup> Research into the eyewitness accounts of bystanders for example, has only partially borne fruit, as the need for effective means of reporting suspicious or threatening behaviors has been identified, but not necessarily implemented.<sup>4</sup>

Clearly, the threat of an Active Shooter incident is of great concern to DHS, but how can such an event be effectively planned and prepared for according to the DHS Risk Management Process?<sup>5</sup>

*(Continued on Page 13)*

<sup>1</sup> U.S. Department of Homeland Security, *Secretary of Homeland Security Janet Napolitano's Third Annual Address on the State of Homeland Security: "The Evolution and Future of Homeland Security"*, February 26, 2013, (Washington, DC: Office of the Secretary). Transcript of the press conference can be found at: <http://www.dhs.gov/news/2013/02/26/secretary-homeland-security-janet-napolitano%E2%80%99s-third-annual-address-state-homeland>.

<sup>2</sup> U.S. Department of Homeland Security, *Active Shooter: How to Respond*, (Washington, DC: The Department of Homeland Security, October 2008), at 1.

<sup>3</sup> Diana A. Drysdale, William Modzeleski, Andre B. Simons, *Campus Attacks: Targeted Violence Affecting Institutions of Higher Education*, (Washington, DC: United States Secret Service, United States Department of Education, Federal Bureau of Investigation, April 2010), at 18, can be found at: <http://www.secretservice.gov/ntac/CampusAttacks041610.pdf>.

<sup>4</sup> William S. Pollack, William Modzeleski, Georgeann Rooney, *Prior Knowledge of Potential School-Based Violence: Information Students Learn May Prevent A Targeted Attack*, (Washington, DC: United States Secret Service & United States Department of Education, 2008), at 9, can be found at: [http://www.secretservice.gov/ntac/bystander\\_study.pdf](http://www.secretservice.gov/ntac/bystander_study.pdf).

<sup>5</sup> U.S. Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, (Washington, DC: National Protection and Programs Directorate, April 2011), at 15.

(Continued from Page 12)

Current efforts focus on training and awareness, and some external organizations, such as the NRA, advocate the posting of armed security at schools and other soft targets.<sup>6</sup> While the need for training and awareness is undisputed, and may indeed save lives in the future, other proposed measures, such as arming volunteers, are controversial and introduce inherent dangers of their own.

Within DHS, the Science & Technology Directorate is tasked with identifying and integrating technologies that can be used to bridge gaps in capability, especially through the use of low-cost civilian off-the-shelf technologies (COTS). Active Shooter detection and prevention is one such capability gap, and a number of emerging, low-cost technologies have been identified that could successfully address the problem.

One solution to consider is to equip security and volunteers at soft facilities with head-mounted display (HMD) systems such as Google Glass.<sup>7</sup> These HMD systems are wearable computers featuring an augmented-reality head-mounted display (typically over one eye), equipped with voice recognition and smartphone operating systems. Lightweight and easy to interface with, these devices can transform users into remote surveillance platforms, and many of them for a

fraction of the cost of traditional surveillance systems. Funding for HMD systems at the state and local level could be facilitated through the National Preparedness Grant Program (NPGP) and programs within the DHS Science & Technology Directorate designed to help identify and implement key technologies.<sup>8</sup>

The Google Glass hardware, and that of its competitors, is commercially available, or soon will be, and DHS could request specialized modifications to the software (the hardware is already lightweight, robust, and inexpensive). While typical consumer versions enhance daily activities, the software for a DHS version would include all manner of DHS-related functionality, from emergency and first-response (imagine a first-responder interfacing with a victim, all the while critical information being unobtrusively displayed, responding to voice command), to security and surveillance.

Algorithms can be developed to identify potential Active Shooter perpetrators according to a wide range of biometric and behavioral criteria, as well as instant suspect identification for those already in the system. When potential Active Shooter perpetrators are visually detected, either automatically by the system or manually by the user, the system highlights the threat

and alerts the user in the display field, and simultaneously alerts facility security and administration. Within seconds, depending on the estimated threat level, the facility can be locked down, critical points secured, and in many cases without disrupting internal operations, depending on the response level dictated by facility administration.

In addition to immediate threat detection and enhanced emergency response, deployed HMD systems will continuously stream live audio/video to facility operators, which then upload to DHS collection sites or Fusion Centers. In this way, DHS becomes an active collector of intelligence, effectively bridging the gap between state and federal agencies, as well as greatly augmenting the domestic collection capability of the U.S. intelligence community. According to the 2009 Bottom-up Review, one of the goals of DHS is to create an integrated departmental information sharing architecture, capable of fusing intelligence and law enforcement data across organizations.<sup>9</sup>

It is envisioned that in addition to typical civilian soft targets such as schools, shopping malls, and large commercial buildings, the program will also include hospitals, law enforcement, emergency and first responders, airport and transportation facilities, and any

(Continued on Page 14)

<sup>6</sup> The National Rifle Association, *NRA Press Conference, December 21, 2012*. Wayne LaPierre, (Washington, D.C.: The National Rifle Association). Transcript of the speech can be found at: [http://home.nra.org/pdf/Transcript\\_PDF.pdf](http://home.nra.org/pdf/Transcript_PDF.pdf).

<sup>7</sup> *Google Glass*. More information on the product can be found at: <http://www.google.com/glass/start/>.

<sup>8</sup> U.S. Department of Homeland Security, *FY 2013 Budget in Brief*, (Washington, D.C.: Office of the Secretary), at 6, can be found at: <http://www.dhs.gov/dhs-budget>.

<sup>9</sup> U.S. Department of Homeland Security, *Bottom-Up Review Report*, (Washington, D.C.: Office of the Secretary, July 2010), at 9, can be found at: <http://www.dhs.gov/strategic-plan-fiscal-years-fy-2012-2016>.

(Continued from Page 13)

other facility under the purview of DHS and state emergency and law enforcement. Even port facilities could be served, significantly improving security and customs enforcement through greatly enhanced capabilities of DHS and port operators. Imagine the 9/11 hijackers trying to slip through such a system; they would be forced to look face to face with at least a dozen HMD-equipped DHS personnel before making it to the gate, each time having their face and biometrics scanned by the system.

With tens of thousands of HMD users, generating continuous feed, DHS can not only help prevent Active Shooter and other violent events or emergencies in the short term, but through exploitation of Big Data, this collected material can be used to evolve DHS understanding of Active Shooter events as well as a whole host of security and disaster-related incidents. In the event that a HMD-equipped officer witnesses an event that evolves into a full-scale Active Shooter incident, that entire process will be recorded first hand, in much greater and more immediate detail than currently possible through traditional surveillance systems. Since the system is guided by the user (as well as simultaneously recording everything in the system's field of view), a distinctly human perspective is added to the record, which is often unavailable, either due to the tragic outcome of the event, or the unreliable (and

often untrained) nature of the witnesses' account. Professional analysts, from behavioral specialists to law enforcement and security specialists, will be able to review the record as if they had witnessed the event first hand. Additionally, while the potential for Big Data extraction is greater than the scope of this paper allows, imagine being able to identify specific behaviors or other markers that could be used to further train the detection algorithms, refine the search parameters, and add precious seconds to the response time of the next Active Shooter event.

Aside from the immediate value of recording events from an observer's perspective and alerting security, there is the additional benefit of the increased psychological impact and deterrent effect of HMD-equipped DHS personnel on observed populations.<sup>10</sup> Just as motorists slow down when they see highway patrol, so do people behave more lawfully when law enforcement personnel are present. In this case, the addition of the conspicuous head-mounted camera and computer system will convey perceptions of omniscience on the part of the law enforcer, thus greatly enhancing the capability of that individual to enforce and protect. Even unarmed, security or volunteers (marked somehow, even by a T-shirt labeled 'Security') will maintain a more potent and vigilant aura to potential perpetrators.

It is envisioned that the implementation of such a system

across a wide spectrum of soft targets and critical infrastructure will not only decrease Active Shooter incidents, but all manner of criminal behavior as well. For even if the HMD-equipped user didn't directly perceive a potential perpetrator, how is that suspect to know that the HMD system did not see him? Finally, this system, and its attendant scanning algorithms can be integrated with UAV surveillance systems and other remote monitoring systems, providing an umbrella of integrated surveillance and intelligence platforms. Imagine a DHS operator at a facility a thousand miles away, remotely guiding the camera and detection systems on the HMD unit, the wearer like a human UAV. While some may argue the Orwellian implications of such a system, the potential benefit to public safety and national security is undeniable. DHS 3.0 is well-equipped to tackle these challenges, and hopefully soon Active Shooter will be added to the list of well-managed risks. ❖

<sup>10</sup> U.S. Department of Homeland Security, *Risk Steering Committee, DHS Risk Lexicon*, (Washington, DC: National Protection and Programs Directorate, September 2010), at 11, can be found at: <http://www.dhs.gov/dhs-risk-lexicon>.

# Understanding and Preventing Attacks on Government Facilities by Mentally Disturbed Individuals

by Ed Jopeck,\* Aaron Alford, Ph.D.,\*\* and Kelly Shaffer\*\*\*

As the United States mourns the victims of the latest mass murders in Connecticut and Colorado, concerned individuals in all walks of life have engaged in an emotional effort to understand why such attacks occur and to take steps to reduce the frequency and severity of future tragedies. While much of the debate has centered on the issue of gun control at a state and national level, less attention has been focused on reducing the security risks of attacks at the facility level. The perception that attacks by mentally ill offenders are random, senseless, and occur without warning serves to impede attempts to understand and prevent them through the application of threat appropriate countermeasures. Therefore, this article seeks to stimulate awareness and understanding of threats and attacks by mentally ill individuals and suggests a risk-based approach to considering countermeasures selection at the government facility level.

While it is beyond the scope of this article to present a comprehensive risk analysis of all mass murders and Active Shooters in society, it is possible to look at threats and attacks on government facilities by disturbed individuals as an example of how risks can be assessed and prevention and response measures can be selected. This discussion is particularly relevant for security professionals at government

buildings and other high visibility/high risk locations. A sample of recent and notable attacks on government facilities is provided in the accompanying text box as a reminder of the types of incidents that have occurred at some government facilities.

## Examples of Attacks on Government Facilities

- Carl Campbell shot at three people at a Pentagon bus stop in 1991 and killed a U.S. Navy commander after being turned away from the Pentagon in his attempt to meet with Colin Powell. Prior to the attack, Campbell had been institutionalized and treated for paranoid schizophrenia.
- Mir Aimal Kasi shot at drivers entering CIA headquarters in 1993, killing two and wounding three. Relatives described Kasi as unpredictable and a loner.
- Francisco Martin Duran fired a semi-automatic rifle at the White House from the sidewalk in 1994 (no one was injured). Duran suffered from hallucinations and voices inside his head. Government psychiatrists reported that Duran suffered from a personality disorder, although other mental health specialists said he showed symptoms of paranoid schizophrenia.
- Frank Eugene Corder crashed a stolen Cessna 150 aircraft onto the south lawn of the White House in September 1994, killing himself while apparently trying to crash the plane into the building.
- Russell Eugene Weston shot and killed two Capitol police officers at the U.S. Capitol Building in 1998. Weston had a long history of mental illness which included stints in mental health facilities for paranoid schizophrenia. Prior to the shooting, Weston was released from a mental health facility in Montana where he reportedly claimed to have been brainwashed by the government.
- Michael Kennedy attacked a Fairfax County police station in McLean, VA on May 8, 2006, killing an officer and a detective only a month after escaping from a Rockville, MD mental health facility.
- Andrew Joseph Stack crashed a small aircraft into the IRS building in Austin, TX in 2010, killing himself and two others and injuring 13 people.
- Yonathan Melaku pled guilty to firing several shots at the Marine Corps Museum, the Pentagon, and a military recruiting station in 2010. Melaku reportedly suffered from schizophrenia and was angry over the wars in Iraq and Afghanistan.
- John Patrick Bedell opened fire at the Pentagon entrance in 2010, wounding two officers before being fatally shot. Bedell had symptoms of paranoid schizophrenia, repeated stints in mental health facilities, and a history of drug use.

## Understanding Individuals Who Call, Write, Visit (and Sometimes Attack) Government Facilities

Mentally disturbed individuals have long come to Washington, D.C. with the intent of gaining access to U.S. government offices

*(Continued on Page 16)*

(Continued from Page 15)

and officials. On April 21, 1835, D.C. newspaper *The Intelligencer* observed, “It is a notorious fact that this city, being at the seat of government, is liable to be visited by more than its proportion of insane persons.”<sup>1</sup> It is not surprising that nearly 18 decades later, government organizations are still grappling with this phenomenon. Moreover, both the frequency and severity of such attacks appears to have increased dramatically since the 1980s. During this period, reduced funding for mental health facilities combined with a general policy of de-institutionalization have left many severely mentally ill persons without the mental health services they need. As a result, individuals who in the past would have been committed to a hospital have remained in the community untreated – even though some pose a danger to themselves or others.

In the past few decades, threats by the mentally ill against federal offices or officials have been increasingly well-studied. The security and mental health community’s understanding of criminal psychology has also greatly improved. In the early stages of research, studies focused on the tendency of psychotic individuals approaching government and political entities – usually the President of

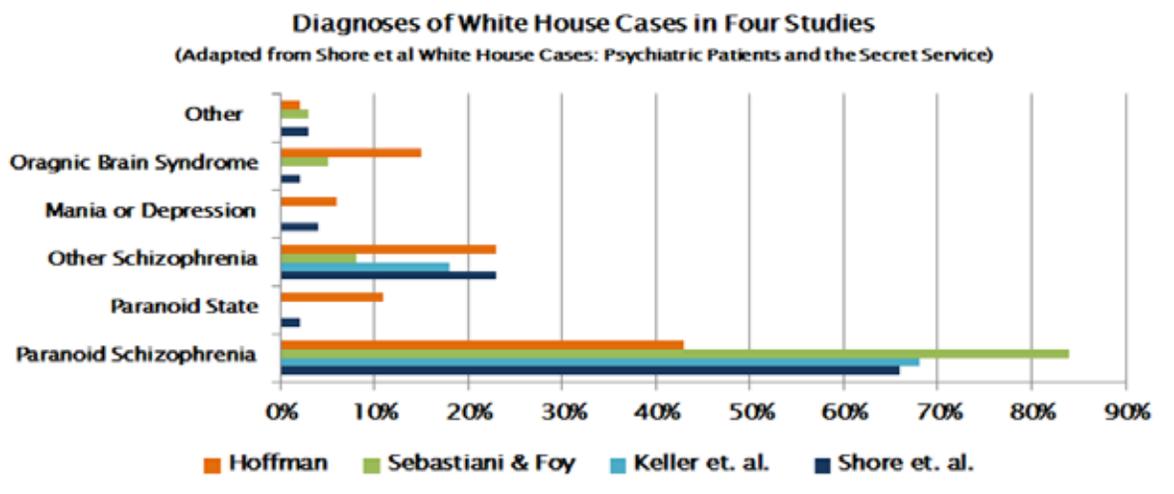
the United States. At the time, such subjects were readily available to mental health researchers because they were committed to St. Elizabeth’s Hospital and/or had been thoroughly investigated by the U.S. Secret Service. These individuals, commonly called “White House cases,” were not significantly different from attackers of other governmental entities and members of the public, but were studied in greater detail because of their availability and notoriety. From these studies it was determined that while acknowledging that the presence of a mental illness does not in and of itself make someone more prone to violence, some features of diagnosed mental illnesses are highly correlated with threatening and otherwise disturbing or inappropriate approaches to government facilities. A compilation of the results of four studies of White House cases clearly demonstrated some forms of schizophrenia and paranoid schizophrenia are more closely correlated with those who were referred to St. Elizabeth’s by the U.S. Secret Service.

Historically, there has been reluctance

for security professionals to recognize inappropriate and often bizarre communications from mentally disturbed individuals as a safety/security risk because they may not contain a clear threat to harm others. Yet review of the attributes of individuals making these communications can help security professionals better understand and perhaps prevent some future attacks. Historically, indications of the potential for future attacks have been provided in the form of repeated calls, letters, and visits to the target (and those associated with them). Yet correctly interpreting these indications is not simple and requires specialized knowledge and insight.

Some of the most innovative research done in cases where the target of attention is not a U.S. president or the White House has been conducted by Park E. Dietz, M.D., M.P.H., Ph.D. et al. In his study, entitled “Threatening and Otherwise Inappropriate Letters to Members of the United States

(Continued on Page 17)



<sup>1</sup> Hoffman, JL, “Psychotic Visitors to Government Offices in the National Capitol,” Read at a meeting of the *American Psychopathological Association*, Boston, Massachusetts, May 17, 1942.

(Continued from Page 16)

Congress”, Dietz focuses on the thematic content of inappropriate communications as an indicator of the potential for dangerous approaches. (See Graph p.19 for thematic content.) Dietz observed that in the population studied, threateners (those who made clear threats to identified targets) were less likely to pursue encounters than inappropriate letter writers who did not threaten, regardless of the type of threat or the harm threatened.<sup>2</sup> This revelation suggests that organizations requiring a legally prosecutable threat as a minimum threshold for further analysis or intervention may be unintentionally excluding those individuals most likely to approach their protectees and facilities.

Dietz found that threatening and inappropriate communications to members of Congress did not necessarily stem from their positions on controversial issues. Like other public figures and governmental organizations, they were subject to pursuit by mentally disordered persons in search of identity, power, relief and personal contact. He also observed that some of these individuals were known to attack the object of their attention.<sup>3</sup> While the study was not the first to look at mentally disturbed individuals seeking contact with government offices, it was the first to look at such communications for pre-approach indicators. By highlighting the need to record and analyze all inappropri-

ate communications, Dietz helped several government organizations re-focus their efforts on the individuals most likely to approach their target, instead of just those who could be arrested for making a verbal threat.

Those individuals who wrote to members of Congress frequently expressed the belief that the government can or must help rectify their personal problems. Sadly, most of these individuals must have been disappointed, and possibly angered, by the treatment they received at the hands of those who could not or would not help them.

Unfortunately, some organizations who receive bizarre or threatening communications may not even be aware of the risk due to the low priority to which this “crank mail” is relegated. An extraordinary example of this is a string of arsons that occurred in 1993, burning some 200,000 acres in Southern California, causing hundreds of millions of dollars of damage, destroying 1,100 structures and ending three lives. One of the suspects in the case, convicted arsonist and child molester Thomas Lee Larsen, was arrested and charged with mailing a letter containing threats to damage or destroy by means of fire. The 7-page letter, which outlined Larsen’s dislike for federal authorities, was signed only with the pseudonym of “fedbuster.” However, what was most interesting about the letters was that Larsen claimed to have mailed about 100

copies. But authorities were able to identify only 36 people or agencies who acknowledged receiving it.<sup>4</sup>

Threatening and inappropriate communications present a novel paradox to security personnel and researchers alike. The overall research on inappropriate communications has shown that persons who communicate direct threats are less likely to actually approach than those that do not make direct threats in their communications. This makes threats a fairly poor predictive tool in general. However, there is some evidence that this pattern is not true for mentally ill individuals. Inappropriate communications to members of Congress by mentally ill individuals have been found to be more frequent, sent to more institutions/facilities than those sent by persons with no indication of mental illness. These communications also tend to be more incoherent and disorganized. In the same study, mentally ill persons who completed an actual inappropriate approach in person were more likely to have communicated with members of Congress prior to the approach. This suggests that threat information-sharing and collaboration between federal agencies concerning inappropriate communications they receive could increase the likelihood of intercepting approaches by mentally ill persons prior to escalation to an attack.

(Continued on Page 18)

<sup>2</sup> Deitz, PE., et al., Threatening and Otherwise Inappropriate Letters to Members of the United States Congress. *Journal of Forensic Sciences*, 1991b. 36, 5 September: p. 1445-1468.

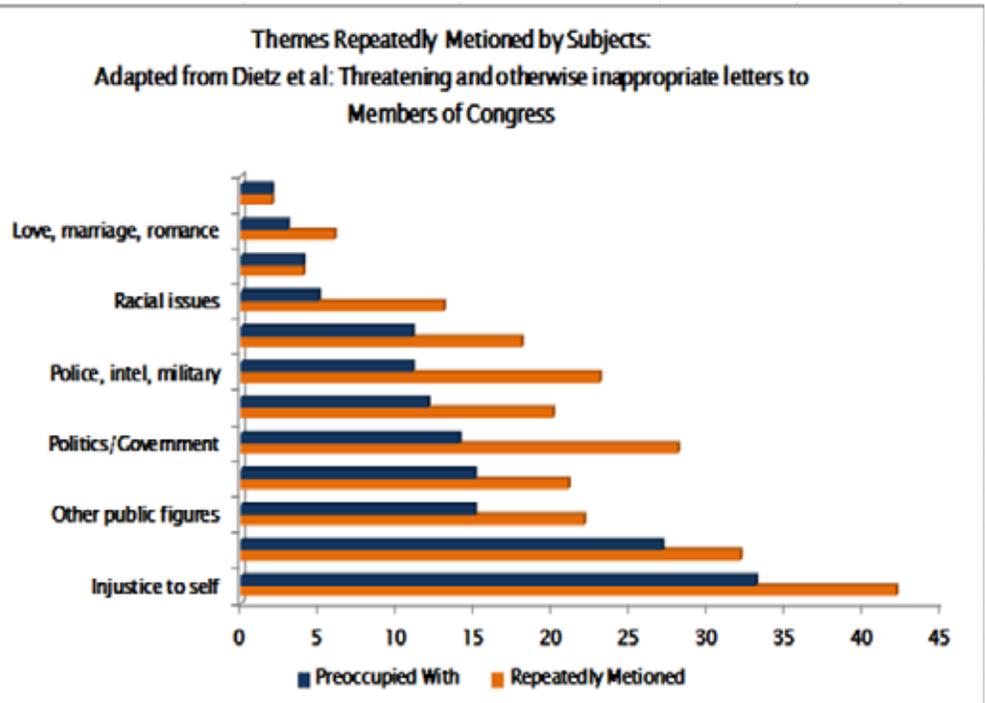
<sup>3</sup> Ibid.

<sup>4</sup> *Los Angeles Times*, date and page unknown.

(Continued from Page 17)

While determining motivation for mental health associated attacks can be a highly speculative venture, if one can draw parallels between what motivates mentally disturbed individuals and what motivates terrorists then the work of H.A.A Cooper may be relevant. Cooper opined that terrorists must feel that they are forced to turn to violence and cross the line when they believe the status quo is worse than the outcomes implicit in acts of violence.<sup>6</sup> This view is supported by statements from attempted assassin Sara Jane Moore, who stated after her arrest for attempting to shoot President Ford in 1974, “I did not want to kill somebody, but there comes a time when the only way you can make a statement is to pick up a gun . . .”<sup>7</sup> If Cooper was right, then understanding what the individual believes and how strongly they feel that the status quo cannot be allowed to continue may be one of the most meaningful indicators of a threat.

Finally, several different threads of research involving attacks on prominent individuals or institutions have shown that even among mentally ill attackers, approaches and assaults are generally the result of a long period of planning.<sup>9</sup> In the words of one research group:



*If an attack occurred, it was a predatory (instrumental, premeditated) mode of violence, rather than an affective (emotional, reactive) mode of violence. Such violence was planned over the course of weeks or months and involved careful preparation and implementation. Approachers and attackers of public figures do not “snap” and are not engaging in spur of the moment, impulsive behaviors. Even if the approacher or attacker is psychotic and severely mentally ill, he demonstrates a capacity and ability to organize his behavior to accomplish his goal.<sup>9</sup>*

This pattern suggests that further research on the patterns, habits, and preferences of mentally ill attackers can shed light on useful and effective strategies against this specific

form of attacker. When applied to the threat analysis of individuals who may pose a risk to an organization or a protectee, analysts should seek to identify indications of planning and preparation for future attacks. These may include the acquisition of a firearm or large amounts of ammunition, travel toward a target, and indications of target research and analysis.

### Countermeasure Strategies

What makes attacks that are the result of mental illness so troublesome to security and protective professionals is the difficulty in preventing such attacks through traditional physical security countermeasures. Target hardening

(Continued on Page 19)

<sup>5</sup> *Supra* note 2, at 1445-1468; Meloy, J. R., et al., A Research Review of Public Figure Threats, Approaches, Attacks, and Assassinations in the United States. *Journal of Forensic Sciences*, 49(5), p.1086-1093, 2004.

<sup>6</sup> Cooper, HAA: What is a Terrorist? A Psychological Perspective. *Legal Medical Quarterly* 1: 8-18, 1977.

<sup>7</sup> Clark JW. American Assassins. Princeton, NJ, *Princeton University Press*, 1982.

<sup>8</sup> James, D. V., et al., The Role of Mental Disorder in Attacks on European Politicians 1990–2004. *Acta Psychiatrica Scandinavica*, 116(5), p. 334-344, 2007; Fein, R. A., & Vossekuil, B., Assassination in the United States. An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approachers. *Journal of Forensic Sciences*, 44, p. 321-333, 1999.

<sup>9</sup> *Ibid.*

(Continued from Page 18)

and the deterrent value of guards and guns have proven to have little effect on mentally disturbed attackers who sometimes undertake such acts as a means of ending their own lives in a highly public forum. Few security professionals would disagree that the White House, the CIA headquarters, and the Pentagon are “hard targets,” yet physical security at these institutions has not prevented recent or deadly attacks by mentally ill individuals acting alone.

For criminal and terrorist acts, the central motivation and intent are well-defined (e.g. the intent of many thefts is to have the use of an object without paying for it. But if they are apprehended acquiring it, not only will they lose possession

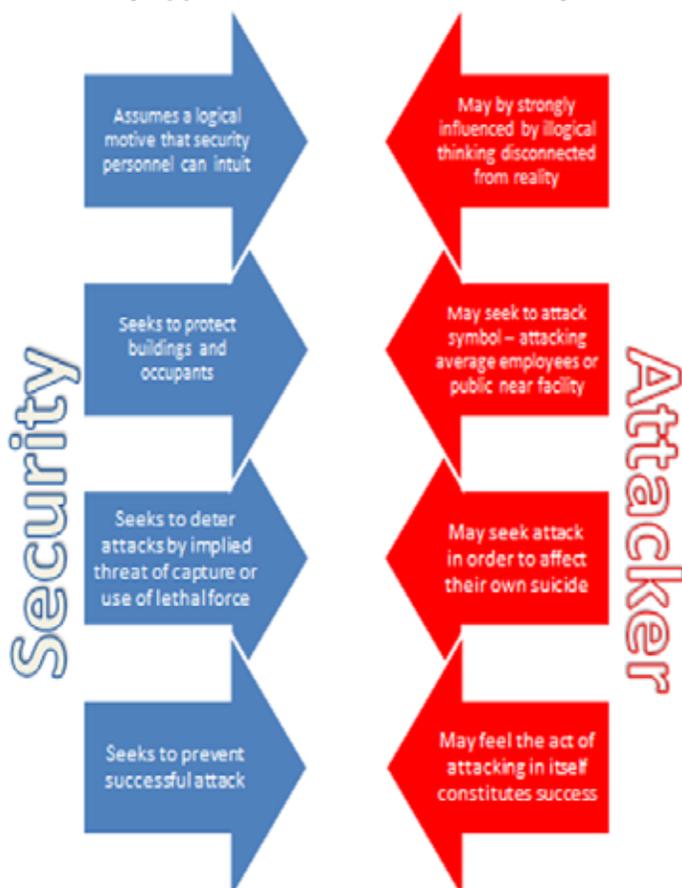
of the stolen goods, but will likely receive some form of punishment). For these acts, security professionals have well-known, common sense approaches to deter such incidents. Consequently, the countermeasures assumed to be effective against terrorists and common criminals may erroneously assumed to be effective against disturbed, often suicidal individuals. The sheer lethality of them may even attract suicidal subjects seeking to commit “suicide by cop.” Thus, a deeper understanding of mentally disturbed attackers is essential to protecting facilities and people from such attacks. Moreover, more analysis of the idiosyncrasies of disturbed attackers could help inform the selection of more effective security strategies and countermeasures to deal with them humanely.

Since the early 1990s, several national security agencies have used security and risk analysis techniques to understand and defend against the full range of terrorist, cyber, foreign intelligence, and criminal threats. A typical risk analysis includes the combination of three subordinate analyses: *threat analysis, vulnerability analysis and consequence analysis*. From these analyses, security analysts learn more about the severity of the threats that they face by researching the intent and capabilities of adversaries who may seek to do harm. When possible, they use this understanding of the threat to preempt attacks and/or disrupt the planning and preparations cycle needed to launch an attack. Likewise, security professionals can direct their analysis inward to understand the vulnerabilities of their facilities, personnel and other assets and make changes that harden the potential targets under their control against the perceived threat. These security countermeasures may deter some attackers from their attempt, or they may only make it more difficult for an attacker to fully succeed if they do attempt an attack. Security professionals, emergency managers, police and other first responders can use the consequence analysis to better understand how to mitigate the outcome of a successful attack that has already occurred.

From a facility security risk management perspective, a risk analysis helps establish a more complete “defense in depth.” This is a security term coined to reflect the concept of layers of security intended to provide multiple methods of

(Continued on Page 20)

### Traditional Security Approach Relative to the Mentally-Disturbed Attacker



(Continued from Page 19)

countering a threat and keeping adversaries at the greatest distance possible from the protected asset or assets. Defense in depth can be applied in both a geographic and time-order sense. Achieving defense in depth to this type of attack provides three distinct opportunities for layered defenses along a time-ordered continuum:

- **First Line of Defense: Detecting and Disrupting Threats.**

Strategies for the detection and preemption of attacks in the planning or preparation phase may help avoid an active shooter situation at the facility. While most difficult, this strategy has the greatest potential to fully prevent loss of life from an Active Shooter situation. It seeks to completely prevent attacks from materializing at the facility due to successful mental health and/or law enforcement interventions far away from the potential target.

- **Second Line of Defense: Reducing Vulnerabilities.**

Security strategies for deterring, detecting and delaying attacks once an individual arrives at a facility can help reduce the number of casualties and other damage from an Active Shooter who does arrive at a protected facility. This strategy may employ any combination of armed guards; quick reaction teams; integrated gunshot detection alerting that can trigger alerts, evacuations, and door closure/lock-down procedures; evacuation and active shooter drills, etc. Should the first line of defense fail, the second

line of defense may be employed, but the potential for loss of life increases dramatically once the armed individual arrives at the facility with the intent to do harm.

- **Third Line of Defense: Reducing Consequences.** Armed with an understanding of the likely outcomes of an Active Shooter or other method of attack, first responders can enact pre-prepared plans to try to evacuate potential victims and speed treatment to the wounded to attempt to reduce the loss of life from the attack. This strategy may employ police and emergency evacuation and medical response drills, resources, and procedures, but is dependent upon the conclusion of an attack to be effective. Hence, it is considered a last line of defense. According to the U.S. Department of Homeland Security, the average police response to an Active Shooter scene is 18 minutes, while the average Active Shooter situation lasts 12.5 minutes.<sup>10</sup> Therefore, the third line of defense, while worthy of inclusion in a strategy, is not suitable by itself as the only response an organization takes to defend its facilities and occupants from an Active Shooter.

With regard to the first line of defense, few approaches and communications encountered by security professionals will warrant a mental health or law enforcement intervention with a disturbed individual. When these do occur, an encounter with a disturbed person should always seek to avoid unintentionally aggravating him or her. It should always be remem-

bered that psychologically disturbed individuals have been known to attack their family members, friends, and randomly selected people after having been mistreated by others from whom they sought help. Intentionally confronting or “playing along” with the delusions or beliefs of a disturbed individual can have harmful effects on others. Thus, it is important that employees be cautioned to show patience and compassion in dealing with disturbed individuals. One objective in dealing with such individuals is to attempt to redirect them back into the mental health system. Whether this redirection actually prevents a future act of violence, or merely provides the individual the treatment they need, the result is likely to be beneficial for the individual, thereby helping alleviate concern for the government facility and public safety in general.

### Summary

Organizations experiencing unwanted and inappropriate communications and attention from mentally disturbed individuals at their facilities should consider taking steps to understand and reduce the risk of potential attacks. While there is no way to reduce the risk completely, a number of common-sense, risk-based strategies can help security organizations better understand and address the risks they face. While more academic research is required to validate and improve these assessment and intervention

(Continued on Page 21)

<sup>10</sup> Charles E. Ergenbright and Sean K. Hubbard, *Defeating the Active Shooter: Applying Facility Upgrades in Order to Mitigate the Effects of Active Shooters in High Occupancy Facilities*, Naval Postgraduate School, p. 5, June 2012. <https://www.hsdl.org/?view&did=718911>.

*(Continued from Page 20)*

methods, the sharing of analytic approaches and best practices can help develop and improve ever more effective prevention strategies. ❖

*\*Ed Jopeck is a Senior Program Manager with Battelle's Center for Applied Risk Management. His work focuses on using security analysis techniques and risk management solutions for the protection and preparedness of high-risk government facilities.*

*\*\*Aaron A. Alford, PhD, MPH, PMP – Dr. Alford is a psychiatric epidemiologist with Battelle's Center for Analytics and Public Health. His work focuses on evaluating efforts to reduce a variety of problem behaviors, including violence.*

*\*\*\*Kelly Shaffer is a Security and Emergency Preparedness Specialist with Battelle's Critical Infrastructure Group supporting Washington*

*Headquarters Services and Pentagon Force Protection Agency.*



## The Center for Infrastructure Protection and Homeland Security Presents: Fatigue Risk Management in Aviation Operations

The Symposium will equip attendees with the knowledge and approaches necessary to effectively fight fatigue in the operational setting. The human physiology of fatigue and the hazards it represents in the workplace will be explored, along with the effective methods and tools to conduct fatigue risk management, mitigate fatigue's negative effects, and enhance public safety.

This one day session will be held May 1, 2013.  
For more information on registration and agenda  
[click here.](#)



The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).