

Threat Assessment: Scholars, Operators, Our Past, Our Future

J. Reid Meloy

Association of Threat Assessment Professionals, 25th Annual Threat Management Conference,
Anaheim, California

I think you know me well enough, Watson, to understand that I am by no means a nervous man. At the same time it is stupidity rather than courage to refuse to recognize danger when it is close upon you.

—Arthur Conan Doyle, *The Final Problem*,
December, 1893

It is a privilege and honor to be able to present the keynote speech to you, my friends and colleagues within the Association of Threat Assessment Professionals, during our 25th anniversary conference. We are a young, vibrant, and growing organization, yet it is hard for me to comprehend that we gathered a quarter century ago to embark on such an important mission: to assess and manage those persons of concern whom we believe pose a threat of targeted violence.

To be honest, I wrestled to find the precise content for this talk, wanting to please the board who invited me, and also to present to almost 800 attendees—a record for this group—a talk that was informative and perhaps inspiring to all. History will be the judge if I have succeeded.

The title reflects my goal: to outline to all of us, both scholars and operators, what we have learned over the past decades, and what the future may hold for us if we continue to steer a thoughtful and vigorous course. We are products of our history, both inherited through our biology and influenced by our environments, but as a friend of mine, Dr. Lee Jaffe said recently, and much more poetically, “we are

Dr. Meloy is a board-certified forensic psychologist (ABPP) and consults on criminal and civil cases throughout the U.S. and Europe. He is a clinical professor of psychiatry at the University of California, San Diego, School of Medicine, and a faculty member of the San Diego Psychoanalytic Center. He is a fellow of the American Academy of Forensic Sciences and is past president of the American Academy of Forensic Psychology. He has received a number of awards and honors, and was the Yochelson Visiting Scholar at Yale University in March, 2015. Dr. Meloy has authored or co-authored over two hundred twenty papers published in peer-reviewed psychiatric and psychological journals, and has authored, co-authored or edited eleven books. He has been conducting research and writing on personality disorder, psychopathy, stalking, narcissism, criminality, mental disorder, and targeted violence for the past twenty-five years. His first book, *The Psychopathic Mind* (Aronson, 1988), was an integration of the biological and psychodynamic understanding of psychopathy. His co-edited book with Drs. Hoffmann and Sheridan, *Stalking, Threatening and Attacking Public Figures* (Oxford University Press, 2008), led to a commissioned study for the National Academy of Sciences on threats toward public figures published in 2011 (www.nap.edu). His most recent book is the *International Handbook of Threat Assessment* (Oxford University Press, 2014). Dr. Stephen White and he created the WAVR-21 (Specialized Training Services, 2007, 2010; www.wavr21.com), a structured professional judgment instrument for targeted workplace violence. Dr. Meloy is a consultant to

the Behavioral Analysis Units of the FBI, Quantico, and is the originator and developer of the TRAP-18 (Terrorist Radicalization Assessment Protocol). He was a member of the Fixated Research Group for the United Kingdom's Home Office concerning threats to the Royal Family and British political figures, and is a consulting member of Work Trauma Services, Inc., headquartered in San Francisco, and Team Psychology and Security in Darmstadt, Germany. He is also a senior editor of the *Journal of Threat Assessment and Management*. He was a technical consultant to the television program *CSI* from its inception in 2001 until its final episode in 2015.

I thank those friends and colleagues who helped me with this talk: Drs. Steve White, Kris Mohandie, Jolee Brunton, Michele Pathé, Gene Deisinger, Kris Kienlen, Laura Guy, Jens Hoffmann, and Troy McEwan. Also Jim Cawood, Ron Tunkel, Andre Simons, Mary Hamilton, Bram van der Meer, and Julie Herrmann. All the final content choices were mine, but if you have any quarrel with anything I've said, you can probably find many of these folks milling around in the lobby. Above all I want to thank my best friend, and very smart and beautiful spouse, Dr. M. J. Meloy. It has been said that behind every great man sits a good woman. I prefer to say that beside every good man stands a great woman.

Correspondence concerning this article should be addressed to J. Reid Meloy, Department of Psychiatry, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093. E-mail: reidmeloy@gmail.com

shaped by our experiences, we are defined by our decisions.”

In the brief time I have here before you, I came to think that painting a broad brush portrait of what we have learned about threat assessment and where we are going was the most important task at hand. Learning, however, is tricky. I didn't want to just cite scientific research, because often it is boring, and can represent the trailing edge of what is already known by the operators in the field, despite the absence of scientific studies. On the other hand, I didn't want to fall into the trap of advancing beliefs about threat assessment which have not survived the test of time, or are just novel and provocative, but are found to be without merit in a few years. So I settled on this question, what are the *big ideas* in threat assessment? Those conventional beliefs and pearls of wisdom that have withstood the challenges of multiple cases in the real world, and those scientific findings that have been cross-validated in a number of settings which are likely to be refined—and endure—into the 21st century.

A parenthetical note before we begin: I have eliminated most references to studies in this talk, knowing that it would be more likely than not that I would forget a particular study and offend the researcher. As most of you know, there is no shortage of narcissistic sensitivities within the threat assessment community, including my own, so in fairness to all, and in the spirit of equanimity, I will single out very little specific research for praise. If however, you recognize your work as having played a role in a particular *big idea*, please privately enjoy the accolades you give yourself.

Violence Is Not Homogeneous

If we define violence as intentional aggression against another which injures or is likely to injure, and stop there, we have failed to comprehend a body of research which is now 80 years old, and began with laboratory experiments with cats: violence in mammals has two modes which are essentially biologically distinctive. The first is affective violence, more popularly known as defensive, reactive, emotional, or impulsive violence; the second is predatory violence, also known as instrumental, premeditated, intended, and most relevant to our context, targeted violence. This distinction

has major threat management consequences, but curiously is ignored in most of the existing violence risk research and instrumentation: the grandmother of actuarials, the VRAG, makes no account of this difference; and the grandfather of structured professional judgment instruments, the HCR-20 V3, does not explicitly discuss it. Whatever the reason for these omissions, the entire field of threat assessment was forged in the furnace of acts of intended or targeted violence—more dangerous and less common than affective violence, a defensive response to a perceived threat, driven by emotions of fear and often anger. Although these distinctions between modes of violence are best considered on a dimension in practice, the science is there, and the lens through which we view this distinction magnifies differences among acts of violence which are operationally critical: for example, a propensity for affective violence can be decreased through the use of medication, whereas predatory violence is untreatable with any known medical intervention. Threat assessment is primarily concerned with identifying and risk mitigating predatory or targeted violence, but also is operationally useful to address other intentional acts, such as threats, bullying, harassment, intimidation, and boundary violations.

There Is Often a Pathway to Violence

This concept was relatively simple, but revolutionary in our field. It promised to give us a map through which we could understand if there was a pathway in a particular case, where was the person on the pathway, what direction was he going, and how quickly was he moving. However, the map is not the territory, and we have learned that each case is different, and sometimes the pathway is only recognized retrospectively, and missed prospectively. But the model endures because it is a good one, although specific research on it is very limited. Newer theory has attached stages to the model, and also has placed the model in the context of other warning behaviors, recognizing that for some individuals, the threat assessment focus may be more useful if such patterns as fixation upon a particular target and identification with other extreme aggressors take priority.

Threat Assessment Is Different From, and Similar to, Violence Risk Assessment

Although threat assessment is a young tributary from an older and wider river we refer to as violence risk assessment, it is both similar and different. Threat assessment is dynamic—it may change day to day, or hour to hour, in each particular case because the person of concern is doing something different, or the situation has changed, or the target is responding to the threat in a certain manner. It is operational—we threat assessors are moving in real time with the person of concern, gathering as much intelligence as possible as we plan and carry out interventions to mitigate risk. And it is often urgent—a person of concern may rapidly emerge within our area of operations and immediately present a high risk—necessitating a rapid but thoughtful response. My friend and colleague Dr. Steve White likes to quote one of the great threat assessors of the 19th century, Wyatt Earp: “you need to take your time in a hurry.”

And there are similarities: both threat assessment and violence risk assessment utilize various professionals, and they both serve the same purpose: to manage the risk of violence. They also may both accumulate evidence over time which changes the assessment and therefore the management of the case. Finally, the consumers of our assessment and management opinions are often not trained in either violence risk or threat assessment; therefore, patience and clarity need to be critical elements in our communication to others.

Threat Assessment and Threat Management Are Dynamically Related

One does not do threat assessment, stop, and then do threat management. When threat assessment is being done, threat management is also in play. They are dynamically related and change each other. For example, a paranoid individual is threatening violence in his workplace, and a decision is made to interview him directly to determine what risk he poses. The interview is done by a member of the team who decides that confrontation of his paranoid beliefs—pointing out to him how absurd they are—is the correct approach. The interview is grossly mismanaged,—although new information has been gathered,—but the risk has in-

creased since the paranoid person is now angrier and more convinced that there is a conspiracy afoot. On a more positive note, a college student has texted an oblique message that his friend should not come to school the next day, the friend considers it leakage and alerts the TAT at the college, and the student is interviewed by a bright and empathic assistant dean to gather more information. What emerges is evidence of a clinically depressed student, which is confirmed by the counseling center when the student accepts a referral and meets with the psychologist, also a member of the team. Intelligence gathering has mitigated risk. As my friend Dr. Ron Schouten has pointed out, the dynamic between threat assessment and management is a Mobius Strip (see Figure 1).

Dynamic Factors Work Best in Threat Assessment

There are static and dynamic factors which correlate with violence risk. Research has repetitively found that static factors—such as age, gender, and a history of violence—work best in the prediction of long term risk of general violence. However, dynamic factors which change, and may be changeable through intervention,—such as psychotic symptoms, retaliatory fantasies, anticipated loss, and use of stimulants—are most salient for short term assessment and risk management of violence, including targeted violence.

Structured Professional Judgment Trumps *Ipsi Dixit*

Ipsi dixit is a Latin term found in legal textbooks which literally means, “he himself said it.” It is sole reliance on personal authority to support one’s opinion.

Q. “What is the basis for your opinion, doctor?”

A. “I am the doctor.”



Figure 1. Mobius strip.

This used to fly in court, but has consistently been found to be less accurate than structured professional judgment in many scientific studies. SPJs provide a standardized and organized format for consideration of most relevant factors in a threat case, and ideally improve as the science of threat assessment develops. SPJs do not render opinions, but they do make sure that relevant factors are not missed in our work, and guard against the fallibility of memory and the hubris of experience. As my friend Dr. Joel Dvoskin likes to say, “if personal experience is so important, why haven’t I broken par after playing golf for 30 years?”

We also need to be careful when we select our structured professional judgment instruments. We should answer three questions: What is the scientific basis for the instrument? What is the outcome we want to measure? And what is my training in the use of this particular SPJ? These questions should guide us in our choice, which in turn, will increase the scientific soundness of our work.

Words of Wisdom for Threat Assessment

Wisdom is the gift of universal insight. Some of it is passed down through generations without any scientific basis, but holds within it a truth that we dare not ignore. Some of it is scientifically rendered, and therefore even more trusting as a source of guidance. Here are some of my favorites which I think are directly applicable to threat assessment:

Precision Can Be the Enemy of Accuracy

Because we often can be more precise, we desire to do so. But this may force others to try to be more precise, and therefore increase the risk of inaccuracy. As one can see from the model in [Figure 2](#), too much precision can render a finding grossly inaccurate, whereas other findings can be accurate without being precise. Strive for accuracy.

Follow the Rules but Think Outside the Box

These are the words of my friend Dr. Kris Mohandie, and represent the joining of our commitment to legal, ethical, and moral behavior with our capacities for creativity and innovation.

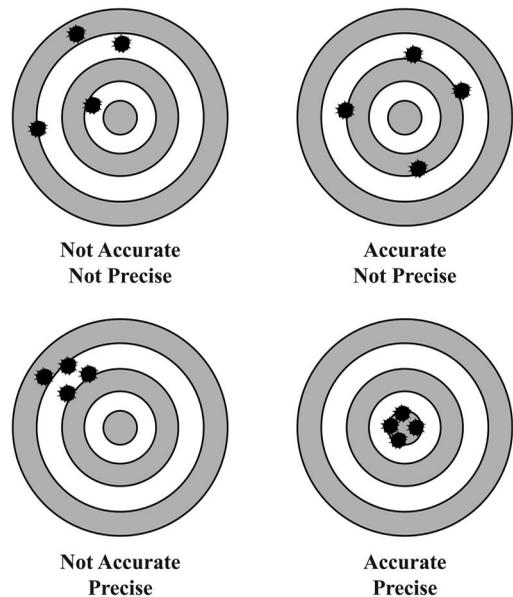


Figure 2. Accuracy and precision.

Your Work Is Their Reputation

This is particularly applicable to the consultants among us, and once again, comes from the spoken wisdom of Dr. Stephen White. His subtlety of language conveys the fact that if we are hired by others, their reputation, in part, is dependent upon our performance. In the psychoanalytic world, we refer to this as the self-object as a source of self esteem. A common experience of the importance of a self-object is the pride we feel as parents when our child succeeds at a certain task.

Monitor Your Own Narcissism

Narcissism—as Dr Arnold Rothstein defined it, “a felt quality of perfection,”—is like blood pressure. Too much or too little is a problem. The paradox regarding narcissism is that the more psychopathological it is, the more likely the narcissist will deny that this is a character or personality problem for him. As an ex-close friend of mine used to say, “when all else fails, devalue those around you.” On a more serious note, Eleanor Roosevelt once said, “You wouldn’t worry so much about what others think of you if you realized how seldom they do.”

Our Recognition of Patterns Is an Evolved Skill Which Helps us Survive Threats

Sometimes we get lost in the details when working a threat case. We do not recognize the forest because we are so intent on a particular tree. Research in threat assessment invites us to step back and see if we can identify patterns of behavior, capitalizing on our hardwired ability to quickly and easily recognize patterns. Here is an example:

How can I read the words with my eyes?

But you just did. Our brain organizes data according to patterns, a phenomenon discovered by the German gestalt psychologists almost a century ago. Pattern analysis now embraces methods including statistical techniques, neural networks, genetic algorithms, fuzzy pattern recognition, machine learning, and hardware implementations; but in our context, it can be simply utilized by attempting to discern a pattern of behavior among the details which we are gathering as a case moves forward in time.

Stalking Has Contributed Much to Threat Assessment for Targeted Violence

An unwanted pattern of pursuit of another which induces fear has contributed much to the science of threat assessment and management for several reasons: as I have written, stalking is an old behavior, but a new crime. Stalking is also a prelude to targeted violence at a frequency that is both disturbingly high, and confirms the legitimacy of this relatively new crime as a means to *prevent* targeted violence. This is no more apparent than the quite shocking statistic—replicated in several cities, countries, and continents—that the *majority* of prior sexually intimate stalkers will be violent toward their victim during the course of stalking. This far exceeds the frequency of violence in virtually all other samples of people at risk for violence, such as short term violence rates of adult males released from psychiatric hospitals who continue to abuse drugs.

Although most stalkers are not psychotic, another finding which has now been replicated in both U.S. and European studies is that the vast majority of those who stalk public figures are psychotic—typically in the range of 80% or more. Stalkers are often both mad and bad.

Criminal Violence Is Decreasing in the U.S., but Mass Murder Is on the Rise

This is a very disturbing phenomenon, but supported by strong research. The FBI Uniform Crime Report has tracked a linear decrease in violent crime in the U.S. over the past 30 years. There have been some intermittently brief increases in some cities, but the general trend is downward over the course of three decades. In contrast, two important studies have recently documented an increase in active shooting incidents and mass murder over the past decade. The FBI found in a 2014 study that such incidents increased 150% if 2000–2006 cases were compared with 2007–2013 cases; and a Harvard Public Health Study, published the same year in *Mother Jones* and shepherded by an excellent investigative reporter, Mark Follman, found that mass shootings between 1982 and 2010 occurred, on average, every 200 days; but increased to *one every 64 days* between 2011 and 2014. Although definitions vary across such studies, these acts of targeted violence, which often victimize strangers in public places, are on the increase. No one knows why, but many think, including me, that social media is an important contributing factor to this disturbing finding, given the appeal of fame, or rather infamy, without achievement—other than successfully killing innocents. The last refuge of narcissistic depletion for the mass murderer becomes “revenge and obliteration,” as my colleague, Dr. James Knoll, has written.

We Face Threats From the Extremes

One of the motivations for such acts is ideological, often couched in a religious, secular, single issue, or psychotic (delusional) belief system. We have historically referred to these individuals as “lone wolves,” and I would like to take a moment to appeal to you to change your descriptive language. The term “lone wolf” has a certain cache, a certain coolness; think for a moment how appealing this term is to an adolescent or young adult male who has, in the words of Tom Friedman, never held a job or a girl’s hand. This becomes, in our shrink terminology, a new identification for him that is very appealing, perhaps a way to define himself—especially if cloaked in secrecy—that may bring with it the most exciting and power-

ful feelings he has felt in years. We unwittingly contribute to these dark identifications by using such terms, especially when we speak to the public or the media, as a number of us in this room do on a regular basis. Language counts, it hurts, and it can even motivate to kill. The same goes for the term, “shooter.” What young man does not find this “sick,” in the parlance of Generation Z? Which one of them would not want to imitate Mark Wahlberg in the film *Shooter*? What young man is not enthralled with first person “shooter” games? Let’s stop romanticizing these terms in the minds of the very few who might be contemplating such acts. Let’s refer to these as “terrorist incidents” or “school shooting incidents,” embracing the three components of threat assessment: perpetrator, victim(s), and situation; rather than fostering a dangerous identity through which a young killer can strike a “cool pose.”

Wherefore Art Thou Mental Illness in Targeted Violence?

Severe mental illness does slightly increase risk of general violence, but other factors are much more important, such as drug use and psychopathy. We know that very few violent crimes are committed by those who are severely mentally ill, but what about targeted violence? Here the research is more ambiguous. One new large study of mass murderers recently appeared in my good friend Dr. Mary Ellen O’Toole’s journal, *Violence and Gender*, and found that about 20% of them were psychotic at the time of the killings. This is curiously comparable to the National Institute of Mental Health’s finding that about 18% of adults will experience mental illness each year in the U.S.—but only 1 in 17 adults live with a severe mental illness. However, mass murder is a very infrequent example of targeted violence. These data points are intriguing, and more research needs to be done; but what is the operational import? Individualize each case. In other words, if there is a mental disorder, what is the relationship, if any, between the symptoms of that mental disorder and a motivation to be intentionally violent? Or does mental disorder play a more indirect role, and destabilize or disinhibit behavior, also increasing risk? Research has shown us that analysis at the level of symptom is often much more important to threat assessment than the diagno-

sis—a fact to which most mental health professionals are oblivious. Mental illness may be an ingredient in the recipe for targeted violence, but at most, it is a small piece of the pie.

Psychopaths Walk the Earth

As Billy Bob Thornton said in his role as a psychopath in the TV series *Fargo*: “there are no saints in the animal kingdom, only breakfast and dinner.” Psychopaths do walk the earth, and unfortunately, commit much of the violent crimes in most societies. In threat assessment, the presence of psychopathy virtually always increases risk of violence, and needs to be accounted for. We all know this, but I want to shine a light on psychopathy that is different from the usual notion, especially among researchers, that it is a psychopathology or a deficiency. Can psychopathy instead be considered an adaptation? In other words, is it a stable genotype in a few humans who were best described by my friend, Dr. Robert Hare, as “intraspecies predators?” I think so. And this is why: many of psychopathy’s traits enhance the success of a predator: low or no anxiety, low autonomic arousal, chronic cortical under-arousal, sensation-seeking, minimal attachment or bonding, fearlessness, calming orientation to a threat, and lessened cognitive load due to an arguable limbic disconnection. This is just a sampling, and unfortunately, I do not have the time to elaborate on each of these points. I would only invite you to not just view psychopathy as a psychopathology or deficiency, but also consider the tactical advantage it confers and the end result: psychopaths do more affective and predatory violence than nonpsychopaths, and no one, despite their optimistic, and in some cases heroic efforts, have found a treatment which works.

Targeted Violence Cannot Be Predicted, yet Can Be Prevented

Targeted violence is a low probability, but high intensity event which cannot be predicted. Yet unless the probability of an event is zero, it will eventually occur. Here is a technical example of the problem of prediction which we face as threat assessors: If 1 of 10,000 people commit homicide, and we apply a risk prediction

instrument that is 90% accurate, there remains a dilemma: Most offenders will be correctly predicted, but for every time we are correct, we will be wrong 9,473 times. This would be the Number Needed to be Detained (personal communication, J. Singh, July, 2015) to successfully capture the one person who would have offended. This curtailment of individual rights, of course, is unacceptable; and we are left with a troubling dilemma. The answer lies in the oftentimes lost distinction between *prediction* and *prevention*. The analogy I use is a cardiologist's medical practice. The doctor may have 500 patients on her caseload that she follows every year, seeing each one on average every 6 months or so. Can she predict which of her patients will have a heart attack over the next year? Of course not. However, she does know the *risk factors* for heart attacks: high blood pressure, obesity, alcohol, tobacco smoke, poor diet, sedentary lifestyle, and untreated prior medical conditions, to name a few. So she practices by addressing the risk factors in all her patients, and if she does this well, the overall rate of heart attacks in her patient population will decrease; and if she is very successful, and can build enough rapport and influence with her patients to comply with her recommendations, the incidence of heart attacks will be better than her comparative sample (national average, state average, other cardiologists' patient populations, etc.). *But she still cannot tell us which one of her patients would have had a heart attack if she hadn't intervened and helped them manage their risk factors.* This is the paradox and beauty of threat assessment; if done well, we will see fewer incidents over time in the population of concern—an arguable example would be the relatively few domestic terrorist acts in the U.S. since 9/11—but we will rarely know if our specific interventions prevented someone from mounting an attack who would have done so in our absence. *Prevention does not require prediction.* We risk manage behaviors of concern in the present and do not concern ourselves with *specific* predictions of future targeted violence.

Watch Your Cognitive Biases

There are many cognitive biases—errors of judgment or choice—that affect normal human behavior. The best read on this subject by far is Daniel Kahneman's 2011 book, *Thinking, Fast*

and Slow, one of the few psychologists to ever win the Nobel Prize. I want to focus on just three which I think are most relevant to threat assessment and management:

First, confirmatory bias. This is our inclination to ignore evidence which does not fit with our theory of the case. Instead of letting the accumulating evidence in an ongoing threat assessment determine our opinions, we ignore evidence which detracts from our predetermined opinions, and highlight evidence which supports our opinions. One insidious way we play out confirmatory bias is to pay more attention to risk factors than we do to protective factors. Confirmatory bias is antithetical to the scientific method in which an hypothesis is developed, and then efforts are made to *disconfirm* it.

Second, availability bias. This is our inclination to ignore statistical probability in the face of an imagined event, such as a feared act of targeted violence, which is emotionally charged and has personal meaning for us. Ten days after 9/11, I flew to FBI headquarters in Washington. As I boarded the plane, the gate agent asked if she could say a prayer for me to ensure my safety. We had a moment of silence together, and I appreciated her heartfelt concern. However, I also knew that despite her fear that my plane would be used as a missile by terrorists, I knew that statistically I was about to travel in an extremely safe manner: not only is air travel the safest means of transport, but 10 days after 9/11 it was clearly the most secure.

And third, predictable world bias. There are two facets to this error in judgment: looking backward or forward with greater certainty than is warranted. Hindsight bias is our belief that an event in the past was more predictable than it actually was. Foresight bias is our belief that an event in the future is more predictable than it is. Plaintiff's attorneys who file civil suits against threat assessment teams will exploit the hindsight bias in a jury by presenting details of the case in retrospect and outside the context of other cases at the time. They will argue, How could this TAT possibly have missed the threat posed by this individual? The job of the defense attorneys in such a case is to develop the context at the time of the assessment. How many other cases were there at the same time which had almost identical risk factors (the signal to noise problem)? How much data that are known now were not integrated at the time by the team due

to the silo effect? The battle for the minds of the jurors is heavily weighted in favor of the plaintiff's attorneys due to hindsight bias.

Foresight bias is just as insidious. We tend to minimize the randomness of events and attribute to them meaning and purpose which do not exist—but this illusion does make such events less anxiety provoking: justice will prevail, it is the will of God, the stock market is predictable, love conquers all. I always wondered how economics can call itself a science when it was virtually unable to predict the Great Recession of 2009. Yet some of us still listen to pundits on CNBC who tell us why the markets went down yesterday, and where they are going to be tomorrow.

Social Media Is Critical to Threat Assessment

There is an old joke that goes like this: How can you tell an extraverted computer geek from an introverted computer geek? The introverted geek looks at his shoes when he is talking to you; the extraverted geek looks at your shoes when talking to you. We are now all geeks. Social media has swept the planet, and is proliferating in both kind and usage every day: emails, blogging, listservs, Facebook, Twitter, YouTube, Tumblr, Instagram, Snapchat, Periscope. There are 300 hours of video uploaded to YouTube *every minute*. It is reported that there are now at least 46,000 Twitter accounts supporting ISIS, mostly inspirational, some command and control.

Friendships have now been redefined by digital hearts; popularity among the young is now measured by number of followers. Within threat assessment, social media now appears to be the most frequently used outlet for the warning behavior of leakage: the communication to a third party of intent to attack a target. Failure to investigate the social media postings of a person of concern is substandard practice.

What do you do if you know nothing about social media? Hire a consultant who is no older than 21 years. I say this somewhat facetiously, but my best resource for what is trending and the current most popular platform is my 11-year-old daughter.

Relevant Philosophical and Scientific Principles

Sometimes larger philosophical and scientific principles help guide us in threat assessment. Here are three of my favorites:

Occam's Razor

Among competing hypotheses, the one with the fewest assumptions is better. Hypothesis One: 9/11 was a Jewish conspiracy orchestrated by the Zionist Operated Government (ZOG) to start a war against Islam, facilitated by the CIA. Hypothesis Two: 9/11 was a terrorist attack by Al Qaeda.

Heisenberg Uncertainty Principle

There is a fundamental limit as to the precision with which we can know something. One of the many hidden ironies in the wonderful TV cable series *Breaking Bad* was that risk-averse Walter White, played by Bryan Cranston, adopted the name Heisenberg when he began his perilous journey into the land of criminality, violence, and uncertainty: "You clearly don't know who you're talking to so let me clue you in. I am not in danger, Skyler. I *am* the danger. A guy opens his door and gets shot, and you think that of me? No! I am the one who knocks!" (Season 4, Episode 5).

The Hawthorne Effect

People change their behavior when they know they are being observed. What are the limits of data in a threat assessment that we can gather from a direct interview? How aggressive should our risk management be? Are collateral data more credible than self-report? This principle brings us back to the dynamic nature of threat assessment and threat management. You do one, you do the other.

Directly Communicated Threats Are on the Stage, but Not the Leading Role

Law enforcement academies have taught for decades that explicit threats are a precursor to violence. Therefore, if there is no threat, there is no problem. Remarkably, this finding has been turned on its head over the past 20 years, first by the U.S. Secret Service Exceptional Case Study

Project. It is now quite clear that directly communicated threats are unusual in targeted violence, for the simple reason that they signal the intent of the attacker and may foil his plan. Not a single person who attacked or assassinated a public figure in the United States between 1949 and 1995 communicated a direct threat to law enforcement or the target beforehand. Very few persons who attacked a Western European politician between 1990 and 2004 communicated a direct threat to the target beforehand. Directly communicated threats are likewise very infrequent in mass murder and active shooting cases, whether adolescents or adults. This discovery originally led to the oversimplified phrase: those who make a threat do not pose a threat, and those who pose a threat do not make a threat. It was further simplified with the distinction between hunters and howlers. Heuristics—shortcuts to learning—are useful, but not always optimal or correct. Sometimes those who directly threaten do attack, especially if the communication is from a prior sexual intimate or current partner. I illustrate this relationship in Figure 3.

Directly communicated threats are the most frequent in sexually intimate relationships and are most correlated with violence risk. This has been referred to as the “intimacy effect.” They are least frequent in public figure cases, and in some studies are negatively correlated with vi-

olence risk. So threats are not as simple as we would like them to be, and in all cases should be taken seriously by the threat assessor.

Leakage Is the Gateway to Many Threat Assessment Cases

Mary Ellen O’Toole and I have defined leakage as the communication to a third party of intent to attack a target—this is a more specific and refined version of the term to distinguish it from other warning behaviors. Special Agent Roger Depue of the FBI was the first person to use this term in the Behavioral Science Unit at Quantico many years ago. The importance of leakage is that it occurs in the majority of cases of targeted violence, such as school shootings, and is often the point of entry into a case for the threat assessor. The limit of leakage is that most of the time it will turn out to be a false positive: there is, in fact, no intent to actually engage in the violence which was communicated to a third party. The promise of leakage is that it is a scientifically sound cornerstone for the “See Something, Say Something” campaigns that have been launched all over the country, beginning with the New York Police Department following 9/11—and such programs have thwarted attacks. In fact, Sandy Hook Promise is rolling out a “Say Something” program for grades K–12 in October of 2015. There are,

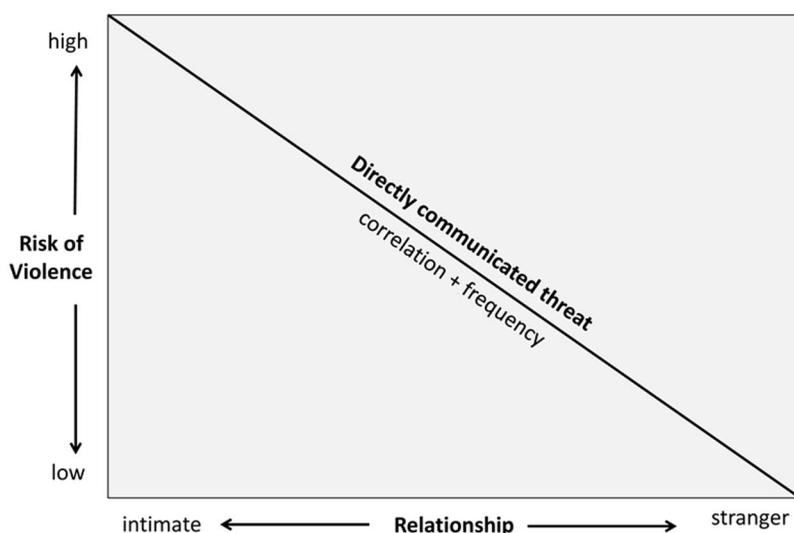


Figure 3. Threats, relationships, and violence: correlational theory.

however, difficulties to still overcome, most notably the hesitancy of people to actually communicate to an authority when they are privy to leakage. Research tells us that we can overcome this so-called “bystander effect” by developing threat management programs where the existence of a TAT is widely known throughout the community, the channel of communication is simple and easily accessible, and the third party trusts the response of the team. Leakage will not tell us who will attack, but it is the gateway behavior which initiates many threat assessments.

Suicide Risk Can Positively Correlate With Homicide Risk

When I was completing my pre- and post-doctoral training in clinical psychology in San Diego, it was the conventional belief that individuals who posed a risk of suicide were less likely to pose a risk of homicide. If a patient was internalizing aggression, they were less likely to externalize it. This turns out to be wrong. Although the vast majority of people who attempt or complete suicide harbor no homicidal intent, a few do. And we must assess for this whenever we clinicians conduct a clinical interview for risk to self. Our hesitancy to do so, however, is evidenced by the extensive research on clinical protocols and structured interviews for suicidal risk, and the paucity of such guidance for homicidal risk. Usually one question is asked in a typical mental health interview, Are you having thoughts of harming others? Check the NO box, go on to the next question. We need to recognize that this is our confirmatory bias: we clinicians want to hold on to this conventional belief that homicidal risk is minimized by suicidal intent, despite the evidence which suggests that they can be positively related. Homicidal and suicidal intent can also rapidly oscillate in the person of concern. For example, we found in a large study that during an encounter that resulted in suicide by cop, there was a 32% chance of injury or death to another person other than the subject in the lethal force incident. When we evaluate for suicidal intent, we must always inquire in a detailed and thoughtful manner concerning homicidal intent.

Psychosis Does Not Necessarily Disorganize Behavior

Another maxim I was taught early in my training was that psychosis disorganizes behavior. It does in some patients, but as threat assessors, this is a question to be answered with each new case: Does the psychosis in this patient disorganize his behavior or not? Catastrophic events have taught us that psychosis, especially fixed and false beliefs such as paranoid delusions, may not disorganize behavior at all. In fact, such beliefs may bring a resolve to commit an act of targeted violence which would be filled with ambivalence but for the presence of the delusions. Jared Loughner. Aaron Alexis. James Holmes; Tucson. The Washington Navy Yard. Aurora, Colorado. These terrible events remind us that psychosis may not disorganize behavior at all. In fact, we found many years ago that psychotic mass murderers typically had a higher casualty rate than nonpsychotic mass murderers. Here is the precise assessment question beyond quibbling about the correct diagnosis: Is there a connection between the delusion and a motivation for being violent? Most importantly we assess at the level of symptom.

Firearms: What Do We Know?

Setting aside the politics of gun control, there are two central facts established by science: Firearms are a weak predictor of violence in general. Firearms are a strong predictor of lethality risk if possessed by a person of concern. In a society where there are as many firearms in circulation as there are people, despite the fact that 99.9% of gun owners are utterly responsible concerning gun safety, the risk is heightened that an individual that we believe poses a threat can easily access a firearm. As a threat assessor, our first priority in any case is to inquire about firearm accessibility or possession, and risk manage by quickly securing such weapons if at all possible. There is also an interesting distinction worth noting here between the enthusiastic gun collector and the person accumulating firearms to carry out an act of targeted violence: the gun enthusiast cannot wait to show his new purchase to his best friend this weekend; the mass murder accumulates his firearms *in secret*. Dr. Randall Collins, a sociologist at the University of Pennsylvania, has blogged about this

important element of secrecy among mass murderers, and how it fuels the emotion of clandestine excitement. This is an important distinction in threat assessment, primarily in areas of the U.S. where gun ownership approaches 100%.

As a gun owner myself, I also believe that firearm ownership, although deeply rooted in our history as a country, and protected by the U.S. Constitution, is a right which is limited, as most rights are—for example, you cannot seriously threaten somebody with violence despite the first amendment protection of your free speech. We should *register* all firearms and their sale; we should *regulate* to keep firearms away from the mentally ill, the criminal, and others who are at great risk to misuse them; and we should *require* demonstrated competency in their use and safe storage before firearms can be owned.

Cultural Scripts for Targeted Violence

Ever since a young man in the throes of chronic catathymia committed suicide in the *Sorrows of Young Werther*, a novel by Goethe published in 18th century Germany, threat assessors from all disciplines have recognized the copycat effect. It appears real, and may become embedded in the culture as a script, a form through which people experience and express meaning. Our most recent example is the Columbine Effect following the mass murder in Colorado in 1999. Recently, *Mother Jones* magazine has documented at least 72 mass murder plots and attacks inspired by Columbine, 21 of which were carried out and killed 89 people. Outside the U.S., this phenomenon is most evident in Germany. Although cultural scripting commands a macro look at one's society, at a case level where most of us live, it means we need to be aware of identifications with previous perpetrators that are uncovered in the person of concern: a desire to be a pseudocommando, fascination with weapons and other military paraphernalia, wanting to imitate previous attackers or assassins, or seeing oneself as an agent or soldier to advance a particular belief system or cause. In case after case, I have seen examples of Mohandie's and my *theme consistency* or *scene specificity* in postevent mass murder reconstructions which hint at the identifications that lie beneath.

The Future

These are the big ideas that bring us to this moment in time. But what of the future for threat assessment and threat management? The science of threat assessment, and particularly threat management, is just beginning, and we have both strengths and vulnerabilities as a specialty.

Our strengths can be found in our emphasis upon multidisciplinary threat assessment teams. The days of the "lone ranger" threat assessor are gone. We know from science studies that teamwork stimulates creativity and innovation, and the convergence of individuals from several disciplines, such as law enforcement and mental health, brings a depth and breadth to understanding and managing a case that would otherwise be absent.

We have also seen tremendous growth in our networking abilities, organizations, a science journal, newsletters, conferences, and meetings. I hope the next step for our networking abilities is a closed listserv through which we can exchange ideas and refer cases, accessible to all members of our 4 sister organizations: the Association of Threat Assessment Professionals, the Canadian Association of Threat Assessment Professionals, the Association of European Threat Assessment Professionals, and the Asia Pacific Association of Threat Assessment Professionals. We also see a proliferation of newsletters from the organizations and allied private companies of our members, posting important conferences, meetings, and trainings in the near future. We now have a peer-reviewed science journal published by the American Psychological Association, *The Journal of Threat Assessment and Threat Management*. Every published article goes into a computer database that is accessed by thousands of researchers, students, and practitioners throughout the world. As we enter our second year of publication, I think we are on the road to success if each of you considers contributing. We need case studies, descriptions of working programs, and opinion pieces, in addition to original research. Please do not be intimidated by our call for your work. Those of us who are the senior editorial staff are happy to help each of you to refine and polish your submissions—and they do burnish your resume.

We also are embarking on certification, and by extension, defining best practices and an evolving standard of practice. Such practical efforts, if done with rigor and honesty, help grow the discipline and the science which shapes it.

And finally, our Code of Conduct, published on the ATAP website, is largely drawn from the American Psychological Association Code of Conduct. It helps keep us on the ethical path and out of the swamp of civil litigation.

What about our vulnerabilities? We need more scientific studies which test many of the big ideas I have advanced today, especially those concerning threat management. We especially need comparative studies and prospective studies so we can actually see what works. We need to pay close attention to our clarity of terminology and our measurement of outcomes. Our colleague Dr. Dewey Cornell at University of Virginia is pioneering the effort to conduct randomized controlled trials of threat assessment and threat management in high schools in Virginia. We need much more work like his throughout our discipline. Thank goodness for the efforts of people like my friend and colleague, Dr. Mario Scalora, who is creating a diaspora of threat assessment forensic psychologists throughout the country, as he mentors new PhDs every year. And Dr. Jim Turner who has carried forward a tradition of honoring new doctors at each of our ATAP conferences through the years. All these efforts help us build an *evidence-based* practice, and win us respect throughout an international community of scholars.

We also need to recognize that there is a stunning lack of understanding of threat assessment and threat management outside our specialty among law enforcement officers, mental health professionals, other corporate and university professionals, and the courts. TATM is typically not taught in any doctoral psychology programs or psychiatry residencies anywhere. This needs to be remedied through our constant efforts to inform and educate. Teach threat assessment whenever you find yourself in a teaching moment.

We also need to watch our vulnerabilities with credentialing: are the methods by which we are conferring a credential reliable and valid? How can we demonstrate this in the unfortunate circumstance—which will eventually happen—that a person who has failed to be credentialed challenges the entire procedure, perhaps in court? I have learned a lot in my training, education, and experience as a forensic psychologist, but probably the most useful personality categorization I ever remembered was in a foreign film: there are three types of persons: leaders, followers, and assassins. As threat assessors, we must stay situationally aware in all we do.

I have walked across a large and varied landscape with you today, and yet one question remains unanswered: why do we do threat assessment? Although each of our motivations vary, I think they coalesce around safety: safety for us, our communities, and above all, our children. Our work, if done well, will speak to the generations to come.