2015

Then and Now: Tracking a Federal Agency's Threat Assessment Activity Through Two Decades With an Eye Toward the Future

Mario Scalora
University of Nebraska-Lincoln, mscalora1@unl.edu

William Zimmerman
United States Capitol Police

Journal of Threat Assessment and Management
2015, Vol. 2, No. 3-4, 268–274

2169-4842/15/$12.00 http://dx.doi.org/10.1037/tam0000057

Then and Now: Tracking a Federal Agency's Threat Assessment Activity Through Two Decades With an Eye Toward the Future

Mario J. Scalora
University of Nebraska-Lincoln

William Zimmerman
United States Capitol Police,
Washington, DC

The following is an edited summary of a plenary session provided by the speakers during the 25th Annual Conference of the Association of Threat Assessment Professionals (ATAP) Conference held August 2015.

The Early Days

We are going to talk a little bit about history. We are sorry to bore you with this again but this is going to be about the history of the Capitol Police Threat Assessment Section. In 1987, the command made a decision to develop a threat assessment unit. We were trying to find out who actually made that command decision but nobody claimed it. We credit our Chief of Police at the time who was James Carvino. The Congress, the Senate, and the Capitol Police were not satisfied with the results that they were getting related to threats against Members of Congress. At that time, the USCP was in the process of starting a dignitary protection division for congressional leadership and so they needed a little bit of justification for spending the money. Like everything else back then, they did it in a really organized fashion as they brought two investigators and a Sergeant together and said, "Ok guys, you are going to take care of threats on Members of Congress." We will tell you that there was not a lot of training on threat assessment and threat management back then. But, as cops the only cases handled then were direct threats like, "I am going to kill you," or "I am going to blow up your building." So we had a lot of stuff going on and our caseload at that time, as you can see, was approximately 300–350 cases. However, Members of Congress' staffers were calling up and saying something to the effect of "Tom Jones just called and said I am going to do everything in my power to make sure that the Congressman is not in office next year." At that time the response would be, "That is not a violation of the law. Call us if something happens." Sadly this was kind of the mentality in the late 1980s. For example, if a battered woman came in and said, "My boyfriend said he is going to kill me if I leave," police would respond we would have to wait for a crime like a direct threat to occur. We are not justifying the mentality back then, but cops then mainly arrested and locked people up. We were just starting threat assessment and did not comprehend threat management. We did not manage threatening people at that time. No-

Mario J. Scalora, Department of Psychology, University of Nebraska-Lincoln; William Zimmerman, United States Capitol Police, Washington, DC.

Dr. Mario Scalora currently serves as a professor of psychology at the University of Nebraska Lincoln. Dr. Scalora has an extensive background as a consultant to various law enforcement agencies at the local, state, and federal levels. He currently serves as a consulting psychologist to the Threat Assessment Section of the United States Capitol Police assisting with case consultation and research activity related to threatening activity toward Members of Congress. He also serves as a threat assessment consultant at the University of Nebraska-Lincoln Police.

Detective William Zimmerman is a retired 32-year veteran in the United States Capitol Police. In 1987 he had been assigned the Threat Assessment Section (TAS) and retired in 2015 as the senior investigator. The TAS is responsible for investigating threats against members of the U.S. Congress, their families, and other statutory protectees. The TAS reviews and evaluates inappropriate contact with members' offices in Washington D.C. as well as offices throughout the United States. Detective Zimmerman conducts training and interviewing, handling and assessing subjects who have come to the attention of the congressional community. Detective Zimmerman also regularly conducts security awareness seminars for the Senate and House staff throughout the United States. He was the first president of the ATAP Washington D.C. chapter in 1994 and currently is their chapter president. Detective Zimmerman is also an ATAP Meritorious Service Award winner.

Correspondence concerning this article should be addressed to Mario J. Scalora, Department of Psychology, University of Nebraska-Lincoln, 238 Burnett Hall, Lincoln, NE 68588-0308. E-mail: mscalora1@unl.edu

body ever thought about the threatening party returning in the future. We made a lot of mistakes because there was not any threat assessment training out there. There was no training to interview the kind of people that we were going to need to manage. When the TAS started, we monitored the radios for a uniformed officer on the Capitol grounds to say something to the effect of "I have got this guy here who thinks satellites are going into his head and he needs to talk to Congress." We would leave the office immediately and started talking to the person of concern. So for the first three years of the TAS's operation, the USCP viewed the "threat guys" as making the mentally ill problem visitors go away. But, we learned how to talk to visitors who had delusional ideas, such as "You know, the government was following me;" "I worked for the CIA since I was three and they owe me a lot of money."

Another problem back then was gaining information quickly on individuals when appropriate. We have Lexus Nexus now, and the private sector has Choice. People believe that the government may have behaved like big brother then but now the Internet exists and you can find out many things about people that are publicly accessible. We used to tell everybody the first thing to is run a criminal check on a subject of concern; now the first thing we do is Google them as you find out a lot more. Threat assessment professionals both love and hate the Internet. The Internet propagates a lot of threatening activity, but it is also a valuable source of information. Getting information from NCIC [National Crime Information Center] can sometimes be challenging as it can only be used for criminal investigations.

Another early challenge was trying to get stakeholders to report behaviors of concern at early stages before problems escalated. About a year after the TAS was formed, we went back to command and proposed something novel at that time. We were going to try and prevent the persons of concern from getting to the point where they were so frustrated or angry that they want to kill or harm someone. One has to understand that with the government, units get more money and more manpower with statistics. So instead of going back at the end of the year and asserting we locked up 150 guys and sent 20 people to the mental hospital, we went to command and asserted we are going try something different and at the end of the year no one will be killed or injured, but we still need more money and resources. Believe it or not, they told us you can do it for a year and then we will evaluate it. Twenty-six years later we are still evaluating and we are still learning. This process has been ever-evolving and ever-changing. It is one of the reasons we keep doing this. You are constantly entertained when you are in the threat assessment field—you cannot make some of this stuff up. So we got out there and we started educating, not only the stakeholders and staff, but we also had to educate other law enforcement agencies that we existed. I mean there are times that we would have an issue in a distant site like in Wyoming, for example, and we would call local law enforcement and say, "Congressman Joe has got a threat, can you cover for me until I can get out there?" The first response we would receive is "Did you guys call the Secret Service?" We had to remind colleagues across the country of lessons learned in 8th grade civic classes regarding the separation of powers. The executive branch protective agency has two main protectees and we have 535. Our colleagues have learned about our agency and we have been very fortunate to receive substantial cooperation over the years when we request assistance.

Concerning another thing that has changed, how many of you remember fax machines? We know there are probably not that many of those around anymore but one of the best things about fax machines was that it used a telephone line. Back then there was no caller ID. It was also really funny if you were trying to maintain early evidence for prosecution as the fax machine print would fade. We learned that the hard way. Also in the past, we couldn't trace a call from the House side of the Capitol to the Senate side of the Capitol let alone try to trace a call outside of Washington, DC. You have to understand the government works with the best equipment available for the cheapest price.

Luckily, in 1991 we learned that there was another unit in the United States that had threats in their name—the LAPD Threat Assessment Unit. We like they had threats in their name as we did, we presumed they have got to know something. So after contacts with the LAPD unit commander John Lane, Zimmerman learned of the local training related to California issues and California law. It seemed like the DC

Chapter of ATAP formed soon after that. If it were not for the DC chapter, ATAP would not be a national organization. ATAP realized there was life outside of California so that is our claim to fame in DC. We had both sides covered, the left coast and the right coast. We cannot emphasize enough how much ATAP and the people that you meet at ATAP have been valuable colleagues and resources. The U.S. Capitol Police is really unique as we do not have field offices across the United States like most Federal agencies do. We rely immensely on local and state law enforcement agencies to help us get though and understand what is going on in their neck of the woods. So it was so beneficial after returning from the second or third ATAP conference and the bosses were saying something like: "We have a case going on in Cleveland and we don't know anybody in Cleveland." Because of the contacts made at the ATAP conference we gained connections that allowed us to move quickly and cooperatively with threat assessment activity. This is especially critical as the USCP not only has to assess risks to the protectee quickly but also determine the need to send protective resources in a timely manner. Detective Zimmerman was able to surprise his command with all of the national connections he was able to develop through national ATAP meetings.

We described how the USCP Threat Assessment Service started. Now, it is a much larger operation. We went from two agents to the current staffing of 16 agents. We have representation on the Electronic Crimes Task Force, the FBI Behavioral Analysis Unit, and the FBI Violent Crime Task Force. So we have come a really, really long way. We can remember when we were all excited about 300 people coming to ATAP national conference and you know we are now pushing over 700 attendees. That is awesome that more people are interested in doing threat assessment. As exemplified by ATAP conferences, we have to keep communicating across disciplines if we wish to continue to move forward. We will now describe some of the trends the USCP encountered.

USCP Threat Assessment Data

The USCP has used Dr. Scalora since the late 1990s to provide case-based and research consultation. The purpose of the research was to evaluate trends in threat assessment activity encountered by the agency, verify relevant risk factors as well as assess the outcome of threat assessment and management activity. Our goal is to share with you a little bit about history and resulting lessons learned. It is also important to not only understand how our knowledge of threat assessment evolved but how those changes of knowledge were spurred by critical events—the USCP is certainly an example of that. Analyzing case trends since the 1980s, you see a spike in threat assessment activity following the Weston shooting at the Capitol in 1998. Our data points out that after a major public incident, although many people will rally around law enforcement and public institutions, individuals who have a grievance against public institutions will actually increase their activity to bring attention to their grievances. Also noteworthy is that after such spikes of threat assessment activity, a new normal in caseloads emerge to a new higher plateau. In addition to inspiring others with grievances, these public events will also get stakeholders to wise up and increase their reporting of concerning behavior. Several other events culminated in increased threat activity within the United States Capitol including: the Clinton impeachment hearings, the 9/11 attacks, and the several Anthrax and Ricin attacks toward Congress. A significant number of cases also emerged during the first (then Senator) Obama candidacy for President. Substantial interagency threat assessment activity and collaboration occurred out of necessity at that time. As the data suggested, increases in threat activity triggered by these high impact public events rarely came back to original threat levels but often settled at new plateau levels. Bottom line is that the agency had to be data aware and data driven in its approach. We constantly looked at the trends because we had to be aware of when the trends might shift to prevent encountering a "big hole in the safety net" given evolution in threat activity.

Another noteworthy trend: Approximately 20% of the cases (and thankfully no more than that) have involved some kind of problematic physical approach toward the protectees or congressional staff. We have been extremely fortunate due to the effort of our agents and our uniform personnel to keep that number at the same level despite increased threat activity.

Regarding additional trends, slightly over four out of 10 people the USCP Threat Assessment Section currently deal with suffer from serious mental illness. Our definition of serious mental illness is that the psychotic symptoms displayed are observable and obvious to a trained investigator. We are not referring to subtle signs of mental illness or persons who suffer from limited levels of emotional disorder that is difficult to observe. We are tracking blatant displays of psychotic symptoms.

We recognize the caveat that persons with mental illness are no more dangerous than the rest of the population. Our statistics show that we have a lot more contact with seriously mentally ill persons of concern and most times it is because they either stopped taking or refused to take medications. We work with families who have been ravaged by the impact of these illnesses. Thankfully the number of cases where such persons have been violent or intercepted by law enforcement or other staff before someone was injured have decreased. We have to take a very sympathetic and respectful approach to them in many respects. One, because it helps manage and move them along to find some resolution and two, because they are coming back. If we are rude or dismissive to them, they are just coming back more angry. Law enforcement had to shift its approach to dealing with mentally ill individuals. Many of these individuals may have frankly been traumatized early in their lives. There are individuals that may have very legitimate issues and sometimes frankly the government has not treated them well. They are not getting the benefits and things they deserve or maybe they have been dismissed and patronized. In many respects, our agents were the first people who actually listened to them with respect or took them seriously while also counseling them to avoid threatening activity.

Regarding other threat assessment trends, the USCP has encountered more threatening communications subsequent to 9/11. Bottom line, people are just less polite and are more threatening in communications toward politicians. There is an increased level of coarseness in communications toward political figures and institutions. We also realize that people are communicating more electronically and they are hitting that send button a little more quickly than they should or they believe that the communication is anonymous. When Anthrax first hit Capitol Hill, the hoax activity exploded to thousands of cases, with several hitting Capitol Hill almost daily. Though true positive incidents are rare, the U.S. Capitol Police has worked hard to maintain awareness of and attention to screening procedures. In addition, we spend a substantial amount of time evaluating electronic communications and making sure that our threat assessment approach is properly accounting for this trend.

Another trend of concern relates to the Internet. More problem communications contain extremist language and by extremist we mean justifying violence to solve political issues. In the past, if people wanted to read extreme doctrine they had to have it mailed and most people had a hard time gaining access. Now they can sit in the comfort of their own home or workplace any time of day and find it rather easily online. More persons are referencing extremist language and it is difficult to determine if they are "card carrying members" of the group or just inspired by its language. We are also finding more people contacting Congress who suffer from serious mental illness citing extremist language. The Internet is also providing supporting networks for individuals who believe they are "targeted individuals." Such individuals have the belief (often delusionally) that the government has picked them out, have them under surveillance, and are making negative things happen to their situation.

As we mentioned earlier, there have been some significant impactful events that have shaped how we have had to look at threat assessment and management. In July of 1998, Russell Weston left his family in Indiana to get to the Ruby Satellite that was kept in the fourth floor of the Capitol that we use to reincarnate people and make clones. So it was a very tragic day—in the aftermath two USCP officers were killed: J.J. Chestnut and John Gibson. What made it even worse was that after the shooting, we put out feelers to all the staff to the places that he lived and asked them to go through and check if there was any previous communications with Weston. We are not playing Monday morning quarterback. Three weeks after the shooting, we got a box from the national archives from offices that had received communications from Russell. When you archive something, whatever you give them is unchanged including the little sticky note that was

still on the letter. The sticky note that said "What do we do with this guy?" was still on the letter. Another note indicated that the communications should be reported to the police. It should be noted that none of the communications contained any threatening language. But we learned that the agencies needed to better share information. The U.S. Secret Service knew about Weston. The FBI knew about Weston. Two state police agencies, at least, knew about him. Numerous local organizations knew about Weston. United States Capitol Police (USCP) was unaware of his behavior. The USCP Threat Assessment Section had been around 11 years and was training for all the congressional offices regarding reporting. The worst part about it was that stakeholders within Capitol Hill did not report the concerning behavior when they could have.

Another thing we learned from the Weston case is that you do not let bad cases drive bad policy. We also learned to look very seriously at what was it about the mental illness that might put somebody at risk to eventually become violent toward one of our stakeholders. We looked extensively at thousands of cases and we found it was not the diagnosis of mental illness per se that drove problem approach activity; it was the nature of the specific symptoms that increased risk. In Weston's case, he suffered from symptoms that suggested malevolent outside forces were causing him harm and causing harm to things he cared about. As a result, he was also displaying other risk factors that we know about. Further, Weston dispersed his grievance across other agencies, and displayed the willingness to travel to express his grievance with these agencies. As a result, these factors suggested a high risk profile. When encountering this cluster of behavior that suggests high risk, we move quickly. We get cases like this at least once a month and many of them when they have been engaged in some travel behavior or moved themselves in closer proximity to our protectees by the time we learn of the concerning behavior. So if there is a silver lining to this case, it forced us to learn about the clustering of these high concern behaviors.

Another significant event of note—the Capitol was among the first with the postal service and some media outlets to receive anthrax and ricin. Seven episodes of confirmed actual biotoxins were delivered to the U.S. Capitol or nearby buildings. We should note that the USCP was aware of bio-terrorism before this. Staff were trained concerning bioterrorism risks and to perform field testing. There were some interesting things that we learned from the bioterror attacks. First was that such attacks were quite possible. We know from the investigation this likely was sent by someone who had access to a highly weaponized and more dangerous version because we didn't expect it to actually go through the weave of the envelope and cross contaminate as well as it did. What were some of the other lessons we learned? No matter how well you train people, cops will rush to the aid of other cops who are exposed to risk. It became critical to make sure the boundaries of the hot zone were rigidly enforced when biotoxins were confirmed. We are not second guessing people here. Nobody dealt with this before. As a result of the act that the boundaries of the potentially impacted area were not initially clear and the information was not shared quickly enough, many thought that they were being vicariously exposed to Anthrax. We learned that the containment zone and management of it had to be tighter—which happened better by episode two.

Also related to the biotoxin attacks was the increased hoax activity that followed. The hoax activity just went through the roof—impacting vigilance of screening activity. As agencies were inundated with thousands of hoaxes, security procedures become lax and we had to learn how to communicate about maintaining vigilance. Peoples' memories of the attacks get shortened because of hoax activity.

In addition to the vigilance issue, which was challenging enough, we learned that certain events may drive activity and inspire people to make more negative contacts that come in waves or clusters. You then have to be prepped for managing and screening waves of problem activity. We then have to look for a pattern of risk activity within the cluster just like we do within an individual threat case. It becomes critical that we make sure we do not let something slip by when managing these activities—highlighting the need to be able to stand up a rapid screening approach when these things happen. Legitimate threatening activities may become part of that wave and can be ignored due to the number of cases to be reviewed.

Increased threatening electronic communications became another trend in threat activity the

USCP observed. We presented here in prior conferences our research related to predictive factors related to electronic communications and our data since have continued to reaffirm these findings. We know from the communications literature that if people communicated electronically they were more likely to be less inhibited, more likely to be threatening, and more likely to be obscene. We also found that when people are communicating electronically they are more likely to throw in more extreme political rhetoric justifying political violence. We found that such extremist rhetoric can come from either domestic or transnational sources. The person of concern himself may not be a Jihadist, for example, but may use some of their threat rhetoric. Although we can theoretically say that the presence of extremist language per se does not mean that a person is a Jihadist, someone sitting in a congressional office somewhere and encountering such language is understandably going to be concerned. Now we have to sort out whether there is a relationship of this extremist language to approach activity. By the way, victims tend to set a different threshold for when they report electronic threats, as they tend to be more tolerant of such activity. If there is a direct threat, recipients are more likely to report, but it is amazing how much electronic threats will pass before they cross the threshold to report—which impacted our outreach activities substantially. Bottom line, several studies have confirmed that the modality of communication is not as important as the pattern of the behavior. As a result, an electronic threat in isolation is not as predictive as the things we see in the rest of the threat assessment literature related to patterns of contact, motivation, and intensity of effort. If subjects are threatening targets electronically and they want to hurt somebody, they are also communicating in other ways. They are displaying other patterns of behavior consistent with other threat literature: personal motive, that intimacy effect, and specific mental illness symptoms. Other content of the messaging such as intention to approach and justified violence language are also predictive. We have also encountered increased communications instigating persons to do violent or disruptive activity. Such activity, especially via tweets and retweets can take on a life of its own. When evaluating such activity we need to stay true to the threat assessment model.

Speaking of being true to the threat assessment model, we have continued to reevaluate our findings though new data sampling to guard against attrition in our effect sizes to make sure that we are not missing certain factors or overplaying certain factors. Bottom line, our findings have been thankfully robust.

A constant challenge remains getting stakeholders to report concerns to facilitate threat assessment activity. We know that people are not likely to report concerning activity to us unless we ask them to do so. For example, we have had to tell our stakeholders that if people are instigating violent activity, please report. Why do we have to encourage people to report? Because they are exposed to many concerning behaviors. We realize we are preaching to the choir of the need for continued education and reminding our stakeholders that it is not a bother to report something. Often stakeholders wait for direct threats before reporting. As we constantly remind people that there is a pathway to violence and we can tie together trends of concerning behavior to gain a better sense of risk posed to prevent problem behavior.

We are seeing a lot more extremist language and we have had to study whether it predicts whether people are going to approach (and we are still looking at it because we are not convinced that the trend cannot shift). Right now our data show that the presence of extremist language by itself doesn't predict anything minus other threat assessment factors. But we have to monitor such extremist rhetoric. It means that we work a lot more with our intelligence units who are more familiar with such extremist language. We also have to educate the intelligence units when to report activity for threat assessment for those same reasons. We have also learned, given recent trends in the terrorism literature, that more persons with serious mental illness are being recruited though Internet-based approaches. Persons do not have to physically attend meetings to learn of extremist doctrine, they can be inspired online. They can literally obtain Al Qaeda's Inspire magazine and learn how to "make a bomb in the kitchen of your mom." We have found more persons who display symptoms of serious mental illness displaying extremist rhetoric. It is concerning for us because we already know that some of the

delusional ideation being encouraged by extremist doctrine may facilitate movement on the pathway to violence. It is sometimes easy to not look past delusional content in communications and note other antigovernment themes found in extremist doctrine (e.g., currency being illegitimate, the government controlling that language, issues against the new world order).

Another challenge facing threat assessment professionals is ascertaining where our responsibilities end when an individual is excluded from a workplace, university, or other institution and is at large within the community. When we are managing cases that are problematic and of high concern, what are our responsibilities to third parties when people leave our doors and how do we share that information? For example, some of our most concerning USCP cases involved expelled college or university students. We are not suggesting universities call us for every disgruntled college student by far but we have had cases of recently expelled college students who were very disgruntled who had a lot of extremist ideation. What do you do if you are a university? What if you do not have a specific threat? Who do you share that with? These are open questions that things we need to think about. Further, where do we go when people do leak information relating to threats (specific or otherwise) to third parties? We have a suspicion that the courts may be defining some of that for us in the near future.

As we touched on earlier, we need to continue to play nice together in the sandbox. We are not operating silos anymore. We have learned the need to share information and talk to other people. We urge everyone here if you are not a member of ATAP to seriously look at it and see where your chapters are locally so that you can go there. The profession will need to continue to work on mechanisms for managing and sharing information within and across institutions related to concerning behavior.

A final note from Dr. Scalora: As a friend and colleague who witnessed much of Detective Zimmerman's service and contribution to the field, it is bittersweet to recognize that he will soon be retiring from the USCP. I want you to join me in thanking him and recognizing his 32 years of service.