Journal of Threat Assessment and Management

Preattack Warning Behaviors in the Digital Space: A Case Study of a Fame-Seeking Rampage Shooter

Mirko Allwinn, Sonja King, Sina Tultschinetski, and Thomas Görgen

Online First Publication, October 31, 2024. https://dx.doi.org/10.1037/tam0000240

AMERICAN PSYCHOLOGICAL ASSOCIATION

Journal of Threat Assessment and Management

ISSN: 2169-4842

https://doi.org/10.1037/tam0000240

Preattack Warning Behaviors in the Digital Space: A Case Study of a Fame-Seeking Rampage Shooter

Mirko Allwinn[1, 2], Sonja King[1], Sina Tultschinetski[3], and Thomas Görgen[2]

[1] Federal Criminal Police Office, Wiesbaden, Hesse, Germany

[2] Department III: Criminal and Legal Sciences, German Police University

[3] Peace Research Institute Frankfurt, Hesse, Germany

Some perpetrators of serious targeted violence publish self-testimonies in the period leading up to their attack, expressing their intention to commit a violent act. This is especially true for so-called "fame seeking mass shooters." This single case study examines whether such materials offer opportunities for threat assessment. For this purpose, publicly available documents of the online activities of an American rampage killer were examined on a large scale for the presence of any warning behaviors using Meloy's et al. (2012) warning behavior typology. The material included posts that had been published on YouTube, Twitter, and a Columbine fan forum long before the crime. Furthermore, there were self-testimonies in the form of audio files and scanned diary pages that he had uploaded immediately before the shooting. Our analyses show that seven out of eight warning behaviors were clearly identifiable from these materials. The potential for making such perpetrator documents usable for threat mitigation is discussed.

Public Significance Statement

The single case study of a fame-seeking mass murderer shows that warning behaviors according to the warning behavior typology repeatedly appeared in the perpetrator's self-testimonies published online. In such expressive cases, risk assessment is possible and opens up opportunities for preventing serious targeted acts of violence. Public online communication of concern should be assessed with the help of artificial intelligence using well-founded risk instruments, taking the legal framework into account.

Keywords: rampage, warning behavior, threat assessment, case study, open source intelligence

Serious acts of targeted violence occur repeatedly in every generation and every decade worldwide, even if their occurrence can be described as rare compared to other crimes such as murder and manslaughter (Allwinn et al., 2019; Liem et al., 2018). They are not a phenomenon of the digital age (Hoffmann & Allwinn, 2016; Westermeyer, 1982), although the spread of digital media appears to have an influence on the frequency and form of such acts (Helfgott, 2015; Surette, 2016). Immediately following such acts, such as in Christchurch (New Zealand) and Halle (Germany) in 2019 or in Buffalo (United States) and Uvalde (United States) in 2022, these acts are given high priority in reporting and discussions in the traditional media and social media, thus generating immense attention. Violence has always had a high news value. According to Shoemaker and Cohen (2005), *deviance* (behavior that deviates from the norm—which includes serious acts of violence) and *social significance* (impact on personal or

Mirko Allwinn https://orcid.org/0000-0001-6038-8113

Correspondence concerning this article should be addressed to Mirko Allwinn, Federal Criminal Police Office, Thaerstraße 11, Wiesbaden, Hesse 65193, Germany. Email: mirko.allwinn@bka.bund.de

social life) are the two most important categories of news factors (Robertz & Kahr, 2016).

This certainty of attention is particularly attractive for offenders who are categorized as *fame-seeking mass shooters* (Lankford, 2016). The criteria for fame-seeking mass murderers as proposed by Silva and Greene-Colozzi (2021) are (a) direct statements about becoming famous; (b) seeking media notoriety through submitted legacy tokens; (c) posting on media platforms immediately before or during the incident to capitalize on the interest they plan to receive after the attack; and (d) mentioning role models with a history of violence, including famous fictional figures or actual mass murderers/shooters (p. 27, cf. also Allwinn et al., 2022).

The acts of planning and preparing the crime, the preoccupation with fantasies of violence, and the "pre-fantasized afterglory" (Altmeyer, 2019) can trigger a positively perceived state of tension in the offender, which is referred to as clandestine excitement (Collins, 2014). Particularly these offenders tend to record the thoughts and emotions that accompany them in self-testimonies (Allwinn et al., 2022; Helfgott, 2015; Richards et al., 2019; Ware, 2020), which are also known as *legacy tokens* (Van Brunt, 2016). For instance, a Federal Bureau of Investigation report showed that between 1972 and 2015, the majority of lone offenders went public with self-testimonies (including online, texts/books, or by turning to the public media) in the period prior to their attacks (Richards et al., 2019). These artifacts created by the perpetrator before the crime are designed to explain key aspects of the attack (Silver & Silva, 2022) and range from individual documents or files to extensive data packages. Their main purpose is to influence the anticipated discussion and interpretation of the perpetrator's personality and deeds in order to secure greater attention and supposed fame. To encourage copycat acts, some offenders give advice for future acts (*call-to-arms*; Staudenmaier, 2021; Ware, 2020). Some authors suggest that legacy tokens can have a significant impact on future crime (Berger, 2016; Ware, 2020). For example, the Turner Diaries of the Oklahoma City Bomber influenced over 200 acts (Berger, 2016).

In the digital age and with the increasing influence of social media, the internet is becoming increasingly important for this type of perpetrator, which is particularly common among terrorists, rampage perpetrators, and school shooters (Federal Criminal Police Office et al., 2017; Gill et al., 2017; Richards et al., 2019; Shrestha et al., 2019). The (online) self-testimonies of perpetrators can reveal inner states, illustrate the development and discussion of radical ideas, thoughts, and beliefs, spread propaganda, and (unintentionally) inform about upcoming acts of violence. Some of these perpetrators are very prolific and communicative. Some of them play with their statements and are more or less open about their intentions and preparatory actions—for example, by uploading videos that show the later perpetrator during shooting exercises (e.g., Kauhajoki Finland in 2009; for further examples, see Meloy & O'Toole, 2011), which can be an indicator of threat assessment (National Threat Assessment Center, 2020). Digital traces are also highly relevant in the context of (online) radicalization. Therefore, analyzing social media is highly relevant for state security professionals who are tasked with monitoring and assessing individuals who could pose a threat to the security of society.

With the increasing volume of social media content, the main challenge is to identify information relevant to assess individual threat in the huge data streams while keeping the number of false positives to a minimum. Once a rough prioritization has been made, it is the task of the security actors to assess the threat potential more precisely in order to be able to initiate suitable measures. Structured professional judgment tools from threat management can be particularly useful for this purpose (Allwinn & Böckler, 2021).

The early detection and evaluation of relevant communication is highly relevant for at least two reasons: First, monitoring can serve to enforce the rules of the rule of law on the internet so that violations can be sanctioned. Second, comprehensively informed risk management can help prevent serious violent crimes. Therefore, analyzing the usability of communication and online activity of perpetrators of serious targeted violence is essential in order to increase the chances of early detection, averting danger, and prevention (see also Allwinn & Böckler, 2021).

The present study was conducted with two objectives:

- To describe how warning behaviors can present themselves in the digital space.
- To gain knowledge about whether the content published by potential perpetrators on the

internet alone, without further operational steps taken by police and intelligence services, can be sufficient to determine their risk potential with regard to serious targeted violence.

Method

Data

For the present case study, we conducted an open source intelligence analysis in which we evaluated the usability of digital materials that were made publicly available by a perpetrator against risk assessment instruments; in this case, the warning behavior typology (WBT; Meloy et al., 2012). Open source intelligence refers to the collection and analysis of freely available public information, including news media, gray literature, and social media (Williams & Blum, 2018).

The analysis is designed as a feasibility single case study. It is not possible to make statements about larger populations. Overall, we want to come closer to the goal of analyzing open-source data from persons of concern more quickly and with fewer resources. We used the online material of an offender who previously was the subject of another study in which we analyzed the individual case structure (Allwinn et al., 2022). In line with recent proposals like Lankford and Madfis's (2018), Lankford (2018), and campaigns such as the "No Notoriety" campaign and the "Don't Name Them" movement, neither civil names nor internet accounts of perpetrators or their aliases are used in this text. The perpetrators are referred to by the place of their attack; the subject of the present case study is simply referred to as "the perpetrator" (Allwinn et al., 2022).

The perpetrator presented here is a particularly good example of a fame-seeking mass shooter, which is reflected in repeatedly expressed fantasies about fame and copycats. On June 8, 2017, the 24-year-old shot three colleagues and then himself at the small-town supermarket, where he was employed. He left behind extensive self-produced testimonies and had already communicated extensively on the internet beforehand, particularly on Twitter, where he published over 2.434 posts. He was also active on YouTube, Facebook, and in Columbine fan forums. In a farewell letter, he summed up that the great fame he had dreamed of would probably not be granted to him in his lifetime:

> I was just never meant to be famous while I was alive. I wanted fame, I wanted to be recognized on the street, I wanted to be in movies or have documentaries made about me (or re-enactments with actors); I always dreamed of getting somewhere … but it wasn't meant to happen.

His activities are characterized by blatant hatred, racist statements, violent fantasies, and even murderous comments. He also produced large amounts of written, audio, and video content (Table 1). While the videos were initially humorous in nature, this turned into increasingly dark content from 2015 onward. The sometimes macabre and explicit content mainly revolved around a fictitious group invented by the perpetrator, which essentially consisted of exclusively female characters, including his own female alter ego. Some of his accounts had thousands of subscribers and followers. Shortly before the crime, he published links to several files and data packages via his Twitter account, including individual text documents, a scanned diary, various videos, and audio files. An overview of the sources is shown in Table 1.

The WBT

What is particularly relevant for the prevention of serious targeted acts of violence is how to anticipate whether a person is on a pathway to committing such an act. Scientifically sound findings on warning signals that mark this path and are potentially recognizable to third parties are crucial for risk assessment and prevention. Research has identified various risk factors that can increasingly be observed in the behavior and communication of perpetrators. The WBT (Meloy et al., 2012, 2014) goes beyond a mere description of discrete variables and describes patterns based on Gestalt psychology (e.g., Meloy, 2018; Wertheimer, 1938) in order to help identify behavioral patterns that might indicate an increased risk of committing a serious targeted act of violence. It is intended as an initial approach to assess risk and to structure further operational investigations. Accordingly, warning behavior is defined as behaviors that occur in the run-up to serious targeted violence and are associated with the crime (Meloy et al., 2012). Other terms are also used in the operational field, for example, by the Federal Bureau of Investigation, to describe behaviors that are observable and require action (e.g., "concerning behaviors"; Silver et al., 2018, p. 17ff). In our case, we will not introduce other

Table 1
Overview and Availability of the Data Material Considered

Source	Availability in the run-up to the crime	
	Online (open source)	Offline
Social media (focus on Twitter)[a]		
Main account (since August 2015)	Yes (864 posts)	
Alias account fictional group (since March 2016)	Yes (1,190 posts)	
Alias account 1 (since June 2016)	Yes (253 posts)	
Alias account 2 (since July 2016)	Yes (127 posts)	
Columbine fan forum (since December 2016)	Yes (33 posts)	
Text documents		
Text document 1	June 8, 2017, 4:11 a.m., day of the attack	Yes
Text document 2	June 8, 2017, 4:11 a.m., day of the attack	Yes
Text document 3	June 8, 2017, 4:11 a.m., day of the attack	Yes
Hand-written diary	Since January 2017, single pages from the diary had been published sporadically. The full diary was published online directly before the attack.	Yes
Videos		
Videos/reuploads on YouTube	Unknown	
Video of supermarket	June 8, 2017, 4:11 a.m., day of the attack	Yes
Video of fictional Westborough high school shooting	June 8, 2017, 4:10 a.m., day of the attack	Yes
Audio		
Audio files[b]	June 8, 2017, 4:11 a.m., day of the attack	Yes

[a] The accounts central to the analyses were singled out. Other social media accounts were not examined in more detail as they were considered less important, only very few posts were made, or the publication times were unclear due to reuploads. [b] The audio files selected for the analysis dealt directly with the topic of suicide. Other audio files were not included.

terms as we are only concerned with the WBT according to Meloy et al. (2012).

The WBT is made up of the following eight proximal warning behaviors (see also Meloy, 2018):

1. Pathway warning behavior = research, planning, preparation for, or implementation of an attack.
2. Fixation warning behavior = an increasingly pathological preoccupation with a person or a cause, accompanied by a deterioration in social and/or occupational life.
3. Identification warning behavior = a psychological desire to be a pseudocommando or have a warrior mentality, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause or belief system.
4. Novel aggression warning behavior = an act of violence that appears unrelated to the intended act of concern and is committed for the first time; it is typically done to test the subject's ability to carry out his or her act of violence.
5. Energy burst warning behavior = an increase in the frequency or variety of any noted activities related to the target, even if the activities themselves appear relatively innocuous, usually in the weeks, days, or hours before the attack. Social media activity may increase or decrease during this period of time.
6. Leakage warning behavior = communication to a third party of an intent to do harm to a target through an attack; the third party may be an internet audience and/or any social media audience.
7. Last resort warning behavior = evidence of a "violent action imperative" and/or "time imperative" (cf. Mohandie & Duffy, 1999); it may be a signal of desperation or distress. Often the result of an unexpected triggering event, or one that is anticipated, that involves a loss of love and/or work. The subject believes he/she has no other choice and must act now.
8. Directly communicated threat warning behavior = the communication of a direct threat through any means to the target or law enforcement beforehand.

Some warning behaviors also appear to co-occur more frequently than others; in other cases, it is not always easy to distinguish between them. Furthermore, the warning behaviors are not necessarily considered equivalent in terms of their contribution to risk assessment. For instance, the warning behaviors pathway, identification, and last resort are considered particularly relevant for discrimination between attackers and non-attackers (Meloy, Hoffmann, et al., 2021). Böckler et al. (2020) particularly emphasized the pathway, energy burst, novel aggression, and last resort but not identification. If the prior occurs in a *person of concern*, active case management is recommended, and the risk of violence is considered high.

To date, such instruments have been used to a range of different forms of severe targeted violence, such as school rampages and intimate partner killings (Meloy et al., 2014), attacks on public figures (Hoffmann et al., 2011), rampages by adults (Allwinn et al., 2019; Hoffmann & Allwinn, 2016), so-called rampage drivers (Nitsche et al., 2020), and terrorist individuals and small groups (Böckler et al., 2020; Meloy & Gill, 2016).

Since the WBT was first formally presented (Meloy et al., 2012), positive results have been reported on interrater reliability, criterion validity, discriminant validity, and predictive (postdictive) validity (cf. Meloy, Hoffmann, et al., 2021). The WBT revealed "embraces within its categories most of the universe of warning behaviors in intended and targeted violence" (Meloy, Hoffmann, et al., 2021, p. 63f) and therefore claims *real-world validity* (Meloy, Hoffmann, et al., 2021, p. 64).

Analysis of the Individual Case Using the WBT

Using the WBT (Meloy et al., 2012), we place the online preattack communication and the offender's behavior in a threat-analytical context.

Pathway—Research, Planning, Preparation for, or Implementation of an Attack

In December 2016, the future perpetrator posted a short video sequence on Twitter with the caption "Guns! Beautiful…"—a short video sequence showing him shooting with his mother's handgun. On February 15, 2017, he presented a firearm on Twitter that he had purchased a week earlier (Figure 1), according to his diary entry. On April 2, 2017, he wrote, "Fuck yes, I just bought a shotgun, it will be in my own two hands in a few days" and confirmed receipt a few days later.

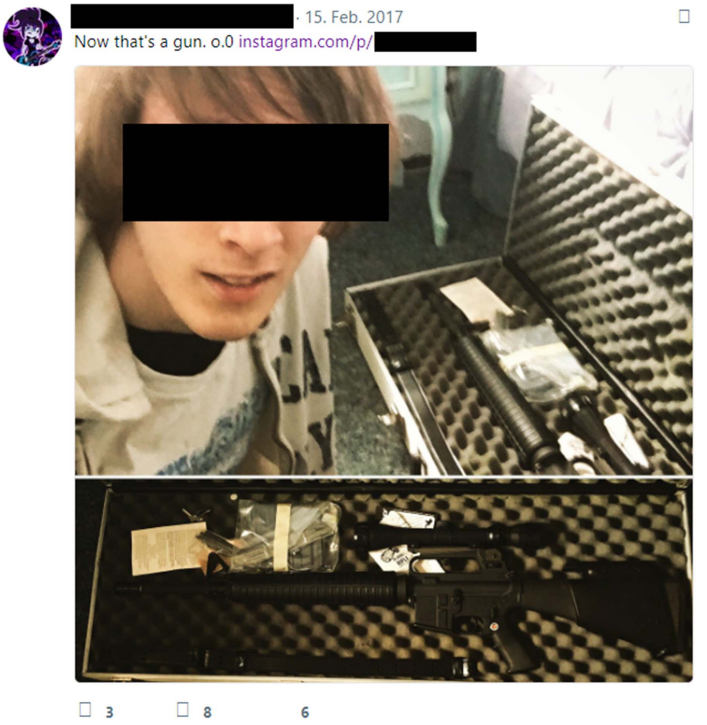
In total, the publicly accessible material documents the acquisition of at least three firearms. He filmed his shooting exercises with these weapons on 7 days between December 2016 and June 2017. He linked the videos on Twitter a few hours before the crime.

In his audio recordings, he described his thoughts about carrying out the crime and speculated on how much time he had until the police arrived. He tried not to post his concrete intentions, planning, and preparatory actions online in order to keep the probability of detection as low as possible. Nevertheless, some information leaked in cross-references between online posts and his offline diary, as exemplified in this Twitter post: "Sometimes it's better to vent in a journal than on the internet" (February 13, 2017, 115 days before the attack) or "There's so much that I want to say that you'll never get to hear until later" (Twitter; February 15, 2017, 113 days before the attack). He finally became more explicit on March 24, 2017 (Twitter; 76 days before the attack), when he posted a photo of his diary and wrote the following: "I write in you almost every day. You are the only set of ears who can know my thoughts. One day I will." On April 11, 2017, he suggested that he would not live until the end of the year: "No more freezing cold winters for me for the rest of time. Finally. You won't be missed" (Twitter; 58 days before the attack). Shortly before the crime, he finally walked through the supermarket again and filmed himself. He called this video "Supermarket Tour (June 7, 2017)—Morning Before the Shooting."

Overall, the pathway warning behavior is fulfilled and up to 6 months visible based on the online material that can be viewed before the crime. We can detect the acquisition and the use of firearms. Even more, he made very clear that his online postings only revealed some of his thoughts, feelings, and plans and that he was recording them in more detail in a diary.

Figure 1

Screenshot of the Twitter Post From February 15, 2017, Showing the Later Perpetrator Presenting His Newly Acquired Firearm



Note. See the online article for the color version of this figure.

Fixation—Pathological Preoccupation With a Person or Cause

In all of his testimonies, a fixation on school shootings, weapons, death, and fame is obvious, and the topics are not characterized negatively. He was particularly fascinated by the shooting at Columbine High and the perpetrators. His Twitter accounts throve on the themes surrounding the fictional group he created, which consisted exclusively of characters who had returned as female ghosts after their unnatural deaths and had the goal of destroying humanity (Allwinn et al., 2022).

These topics (school shootings, weapons, fictional group) were not evaluated negatively and took up a lot of space in his world of thoughts and experiences. Fixation is also fulfilled if it is "accompanied by a deterioration in social and/or occupational life" (Meloy, 2018, p. 13). For example, he wrote, "I can't get guns or Columbine off my mind; I've completely desensitized myself to gun violence." (Journal, p. 83, March 5, 2017, 95 days before the attack).

A morbid fascination with death, which is ultimately seen as desirable, also clearly emerges from the publicly accessible materials. According to the perpetrator, his fascination with death began in 2012 when an acquaintance died in a car accident. In his last recorded audio document from June 1, 2017 ("Goodbye Mom, Dad, Jeremy, and Family"), he said, "Something just broke inside myself … from that point on I was just fascinated by death."

His fixation on fame can be seen, among other things, in the months he spent working on his video production. The media package he left behind contains a text file in which he lists the time spent on individual production cuts for the videos mentioned there. He invested almost a whole year in some of the videos. This illustrates the great importance of video production and how much of his resources he invested in it. Although his social media accounts had a certain reach and

he received a lot of positive feedback—even fan art—that "fame" was obviously not satisfactory to him.

The audio documents he recorded have a playing time of over 17 hr. All these testimonies revolve around his main themes of interest, leaving little room for other content. They express how he devaluated a conventional lifestyle—like starting a family or pursuing a normal profession—and how he could not even imagine growing old.

The proximal warning behavior fixation is therefore fulfilled and could be assessed on the basis of the online material, which was already accessible before the crime or the publication of the media package. The fixation on the central topics went so far that they contributed to a deterioration of his social and professional life. The life he led and growing old were negatively evaluated and rejected, while dying before the age of 30 was glorified.

Identification—Warrior Mentality, Close Association With Weapons or Military Paraphernalia, Identification With Previous Attackers

He repeatedly showed identification warning behavior on Twitter, in a Columbine fan forum on YouTube, in the diary, and in the audio files. For example, he presented himself wearing a white T-shirt with the words "natural selection" in a Twitter post (March 30, 2017, 70 days before the attack).

One of the perpetrators of the school shooting at Columbine High also wore such a T-shirt during the crime, which is why it is considered a meme in the so-called school shooting community. The perpetrator in the given case also presented himself on Twitter (Figure 2) with this T-shirt and wrote, "Who's your favorite serial killer?" with the hashtags (among others) #NaturalSelection, #Columbiner, #Columbinemassacre, and #NBK,

Figure 2
Screenshot of a Twitter Post Showing the Perpetrator Wearing a "Natural Selection" T-Shirt

Note. See the online article for the color version of this figure.

and also mentioned the name of one of the perpetrators of the Columbine shooting (January 5, 2017, 154 days before the attack). NBK stands for the movie Natural Born Killers. This was one of the favorite films of the two Columbine perpetrators. NBK eventually became their code and is a cipher within the Columbine fan subculture. The perpetrator's identification with the Columbine perpetrators was particularly evident in a self-generated hashtag in which he combined the initials of the Columbine perpetrators with those of his own real name and his online alias.

Between December 16, 2016, and July 6, 2017, he also wrote a total of 62 posts in a Columbine fan forum, from which his perceived identification with the perpetrators and the crime becomes comprehensible: "It just sucked me in" (May 21, 2017, 18 days before the attack). The perceived closeness becomes clear in various passages in the online forum in which he expressed assumptions about the perpetrators' afterlife:

> I don't think they're "gone forever." Way I see it is in the afterlife you can still see what happens on Earth but you can't interact. So I won't say [Name] and [Name] don't know about the aftershocks that they've caused. We won't know until we're gone. Someone needs to hire the best medium in the world and have them find [Name] and [Name] souls. (March 3, 2017, 97 days before the attack)

He asked detailed questions in the forum, particularly about the course of the crime, which he sometimes underpinned with expressions along the lines of "I'd kill for it" (February 24, 2017, 104 days before the attack):

> I've always heard they both died at 12:08 p.m. but [Name] was alive longer after shooting himself. … Another theory was they both yelled "ONE! TWO! THREE!" and turned the guns on themselves (which I don't really buy). I think [Name] went first and [Name] took a moment, like in a ritual style (taking off certain accessories).

In one of his posts in the forum, he wondered how often the perpetrators ultimately practiced with the firearms. Some questions show his interest in tactical information and what to look out for from a perpetrator's point of view (February 22, 2017, 106 days before the attack):

> My thoughts would constantly be "how much longer until cops/swat start piling in?" They had no idea that it'd take the SWAT that long to enter. They could've carried on for a while. It wouldn't take much convincing for me to put that gun in my mouth after all of that and just get it over with, thinking they could be out in the hallway about to charge into the room. [Name] without a doubt was instantaneously dead; he practically detached his face from his head. I could only imagine [Name's] reaction though. Like. that's one of the last images you'll ever see in your life; your friend laying in a pool of blood with his face distorted. I'd kill to know what happened in those final few minutes.

His contributions often dealt with the question of what remains of the perpetrators after such a crime. In hindsight, this could point to his own need to leave something behind, which is why he ultimately published his digital set before the crime. In addition to the perpetrators of the Columbine rampage, the perpetrator of the Cleveland Elementary School shooting (San Diego, United States) was also a figure of identification. On Monday, January 29, 1979, the perpetrator fired a sniper rifle from the window of her parents' house at the elementary school opposite, killing four people. She explained her actions to a journalist on the phone and to the police when she was arrested, "I don't like Mondays. This livens up the day" (Janak & Pescara-Kovach, 2017, p. 57). In a post from May 22, 2017, he refers to her with the quote "I don't like Mondays," which makes an identification clear.

He gave his weapons pet names that reflect characters from the fictional group he created. Some photos published on Twitter show him kissing his weapons, symbolizing his close bond with them. It also becomes evident that he considered the fictitious group as some kind of combat unit and himself as a future member. For example, he wrote, "They say God takes young souls because of their purity. … That's a squad recruiting their newest member" (December 11, 2015, 545 days before the attack) or "It may take decades, even a century. You can't beat an eternal army if you're mortal. You will all lose and you will all DIE" (March 19, 2017, 81 days before the attack). He also established a connection between Columbine and the group: "Me and [Alias 1] are going to try and search through dimensions to find [Initials of the Columbine perpetrators]" (November 15, 2016, 205 days before the attack).

In summary, it can be observed that the warning behavior identification is fulfilled. However, differences can also be observed between the various online platforms. His identification as a school shooter is most evident in the Columbine fan forum.

Novel Aggression—Violence Unrelated to the Intended Act of Concern, Committed for the First Time, to Test One's Ability to Carry Out an Act of Violence

Based on the material we reviewed, it was not apparent to us that he displayed novel aggression warning behavior.

Energy Burst—Increase in the Frequency or Variety of Activities Related to the Target

In order to detect an energy burst, we did not focus on the content of the published content but analyzed the development of the frequency of postings. The first thing we noticed was that the perpetrator was active on several accounts, most recently four ones (see Table 1). With regard to his online behavior, in particular the activity of his four main Twitter accounts, there is a difference in the posting frequency between the first months after creating the account and the months close to the time of the crime (Figure 3). The accounts considered here were created by him in the following order: Main Account (August 2015), Group Account (March 2016), Alias 1 Account (June 2016), and Alias 2 Account (July 2016). His diary entries begin in November 2016.

Our analysis shows that the monthly number of his Twitter posts increased almost continuously across the four accounts and especially the year before the crime. We looked at the 3-month average from June 2016, 1 year before the crime. In the months of June 2016, July 2016, and August 2016, he posted an average of 110 times per month across the four accounts. From September to November 2016, the average frequency was 114. In the period from December 2016 to February 2017, the frequency rose to almost 161 posts within a month. Most recently, the number was just under 221 posts (March–May 2017). He committed his crime in the night from June 7 to 8. In the first 8 days of June, he published a total of 68 tweets. If this rate is extrapolated to the entire month, he would have posted 255 tweets within 30 days (Figure 4).

Overall, a gradual increase in the number of posts can be observed within the 7-day period preceding the crime (Figure 5).

Altogether, it can be seen that the perpetrator continuously produced an increasing amount of text as part of his self-testimonies starting in June 2016, combined with misanthropy (Kupper & Meloy, 2021), which will become clear in the section on leakage. He began to document his activities and the events relevant to him, his thoughts, and, in particular, his planning and preparatory actions. This documentation intensified around 3–4 months before the crime and reached another peak within the last few days before the attack. This intensification of his activities can be described as an energy burst of warning behavior, which can be inferred from the observation of his publicly visible postings in the run-up to the crime.

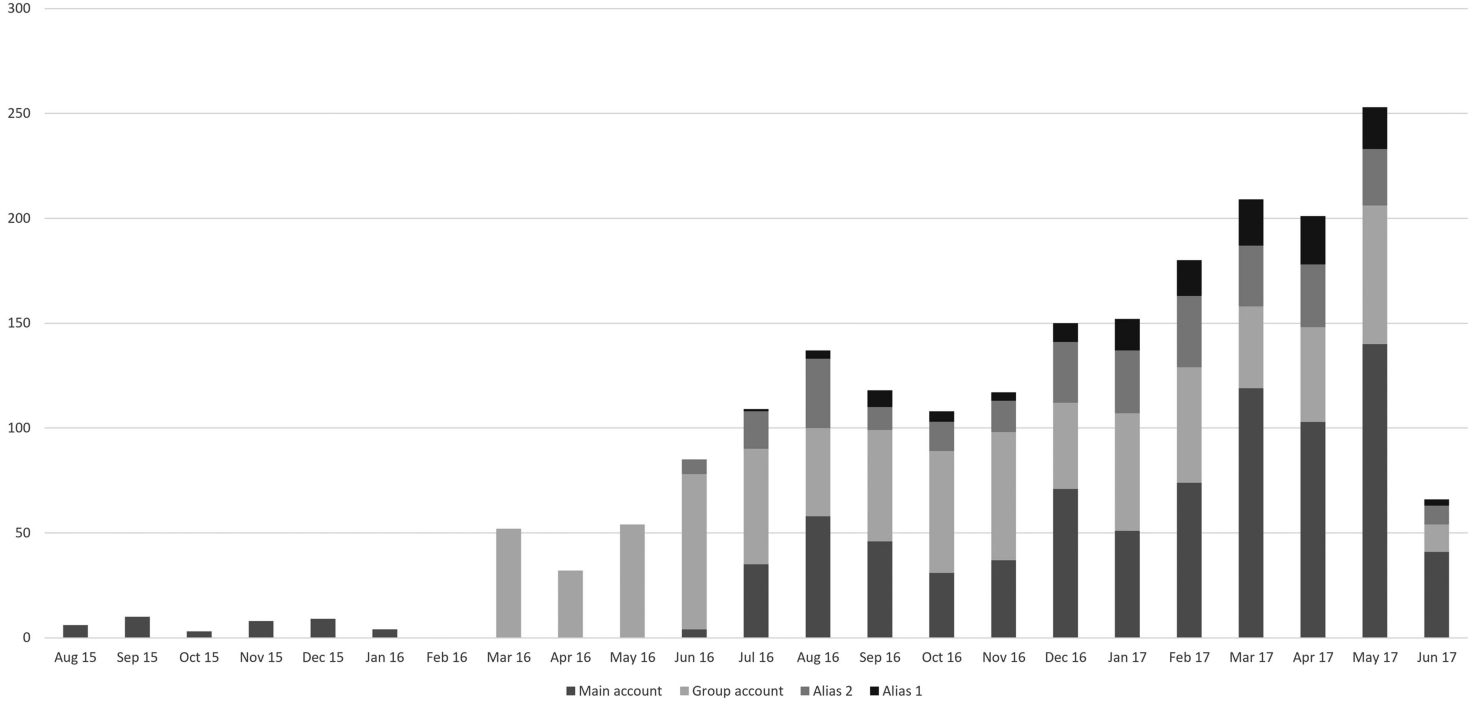
Leakage—Communication to a Third Party of an Intent to do Harm to a Target

The perpetrator showed so-called leakage warning behavior over a long period of time. It began at the latest with the creation of his main account on August 29, 2015, and became even clearer after the introduction of his Alias 2 account. We first look at early leakage statements and then at his statements shortly before the crime.

Early Leakage on Twitter. Almost 2 years before the crime, the future perpetrator made online statements about possible criminal acts. Initially, he considered his high school a possible target. Shortly before the crime, he focused on North Pennsylvania and in particular his workplace. On August 29, 2015, he posted on Twitter: "I feel like spooking some assholes from my high school. #Revenge" (649 days before the attack) and on September 11, 2015: "Floating around my old high school. Analyzing the word's future douche bags." At a later date (September 7, 2016, 274 days before the attack), he tweeted, "One day we'll make worldwide headlines." and continued more explicitly: "School was the most retarded thing ever, so I helped put an end to it … briefly." Based on these tweets, one could conclude that he fantasized about or even planned for his former school to be the potential crime scene. The Alias 2 account is almost universally an example of expressions of the most severe violent fantasies. Finally, 1 day before the crime, the perpetrator uploaded the predominantly animated video entitled "Westborough High School Massacre." It depicts his personal alter ego and this fictional character committing an atrocity at the school of the same name.

He also expressed general fantasies of violence, such as on August 15, 2016: "I'm gonna go to the beach tomorrow and cause someone to drown. I've always wanted to do that … creep

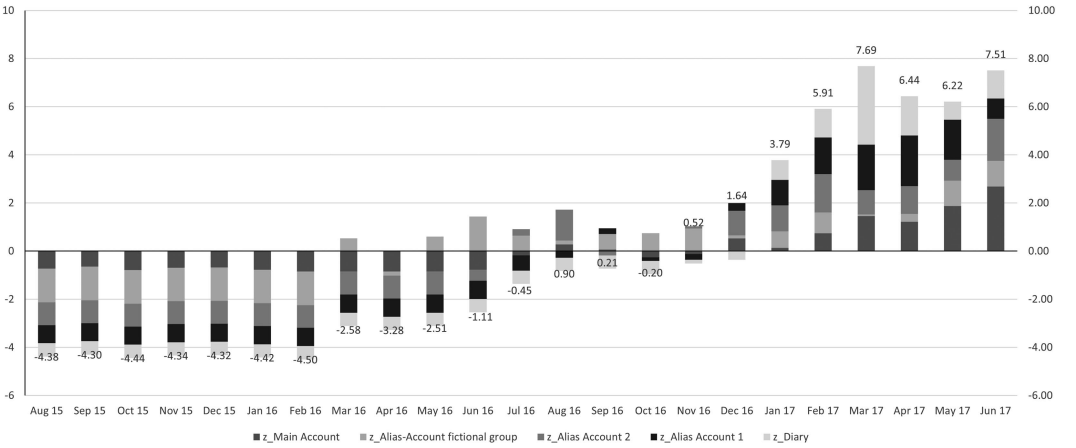
Figure 3
Frequency of Twitter Posts in the Years Leading up to the Attack



Note. The perpetrator committed the crime at the beginning of June 2017. At first glance, the low number of postings in June must be considered in relation to the short period of time. Figure 4 takes into account the number of days.

Figure 4

Standardized Frequency of Twitter Posts and Diary Entries in the Years Leading up to the Attack



Note. The monthly values were first divided by the number of days and then *z*-standardized. The value above the stacked columns is the sum of the respective *z*-values. We relied on the essential and easy-to-record data.

below someone underwater and crab 'em'" (297 days before the attack). On August 19, 2016, he devalued humanity as a whole and used the word "parasite," showing his disgust. He wrote, "We shoot without a gun. We'll take on anyone. You're just a parasite. Now close your eyes and say good night. You better get ready to die!" (293 days before the attack).

Late Leak on Twitter: The Last 3 Months Before the Crime. In the last 3 months before the crime, his leakage warning behavior piled up and became increasingly explicit. On March 3, he mentioned the purchase of a shotgun under "#Goals" (97 days before the attack). On May 20, he posted a countdown: "17 days. … Is your calendar marked? #EGS #BigThings #June7 #DEKHARBS." He wrote about his activities in a Columbine forum and that Columbine had been the most formative event in his life (April 20, 2017, 48 days before the attack). He mentioned flipping a coin to decide whether to commit suicide or homicide–suicide and shared the information that "something insanely huge was decided" (April 25, 2017, 43 days before the attack).

On June 6, 2017, he mostly used his main account to roughly name the region in which he wanted to break down as a force of nature. "If anyone in northeastern Pennsylvania was trapped in that monsoon you have my apologies … #Omen." Finally, he began to say goodbye: "Dude this day is the weirdest day of my 24 years of life. … There's seriously something going on, spiritually" (2 days before the attack). His last post on Twitter before he killed others and eventually himself read: "Goodbye humans. … I'll miss you" (June 7, 2017, a few hours before the attack). At that time, he also linked his media package (June 7, 2017) and sent out a final video link with the comment, "I guess I should finally tell you; tonight's video will be my final production. … I'll tell you why later tonight. There's a lot going on." Finally, he brought his current workplace into focus as a possible crime scene through the video, which he shot in the supermarket and subtitled "Morning Before the Shooting." The specific date of the crime varied across the posts and diary entries.

Overall, the leakage warning behavior is fulfilled very early on based on the online material that can be viewed before the crime. The frequency and quality of the leakage increased over time. Shortly before the crime, the potential time and place of the crime become visible.

Last Resort—Evidence of a "Violent Action Imperative" and/or "Time Imperative," Signals of Desperation or Distress

The perpetrator frequently wrote about the suicide in his own name and in the name of his fictitious group members. In his eyes, the day of death was associated with a rebirth. The term

"deathaversary" appeared frequently in his online statements. On Twitter, he posted a photo with his female alter ego and his fictional soulmate and the words "together forever" (June 7, 2017). He believed that his own death would be followed by real life as a powerful female member of the fictional group. He therefore actually viewed his own death much more positively than his actual life. He posted the model he envisioned for his own suicide shortly before the act (Figure 6). The picture was posted on Twitter with the hashtag "#Heroes" the day before the crime and was liked 125 times, retweeted 67 times, and commented on 25 times.

Statements on Twitter were also noticeable as early as December 2015: "It's weird not having to think about getting older with the new year arriving … #ForeverYoung" (December 31, 2015, 525 days before the attack). He wanted to die before the age of 30, which is why haste was necessary and represented a time imperative (Mohandie & Duffy, 1999). At the same time, he evaluated his life on earth as torture and imagined an alternative reality that he assumed would have far more to offer to him.

His despair and suicidal tendencies became evident in many of his Twitter posts. He wrote about sleeping permanently, no longer being on earth, sitting alone in a dark room, and wanting to listen to horror music on an endless loop. He also discussed taking his own life and wrote, for example, about wanting to shoot his head off. First indications of suicidal tendencies could be found shortly after the start of the main account in the beginning of December 2015: "I had to die in order to live" (December 4, 2015, 552 days before the attack). A look in his diary would have revealed the names of the people he wanted to send his suicide note to and planned to pass on his belongings. There, he also described his wish that his dead body should be photographed and made available to his fans to prove that it is not a fake. Finally, he took his mother out to eat at a restaurant. He had never done this before. This behavior is also a so-called farewell act (Calhoun & Weston, 2015). He hinted at his death on Twitter (March 20, 2017, 80 days before the attack): "I look at Twitter and just want to kill myself even faster. This generation has zero hope left for it." In the last selfie, he looked emaciated (Figure 7). He posted the photo on Instagram with the words, "I hate this place" (June 7, 2017). The bones in his shoulder and hand were protruding. He had recently lost a lot of weight and had probably hardly eaten, if at all.

The publicly available online material initially provided more subtle impressions but became increasingly clear as the date of the

Figure 5
Perpetrators Online Posts in the Week Leading up to His Attack

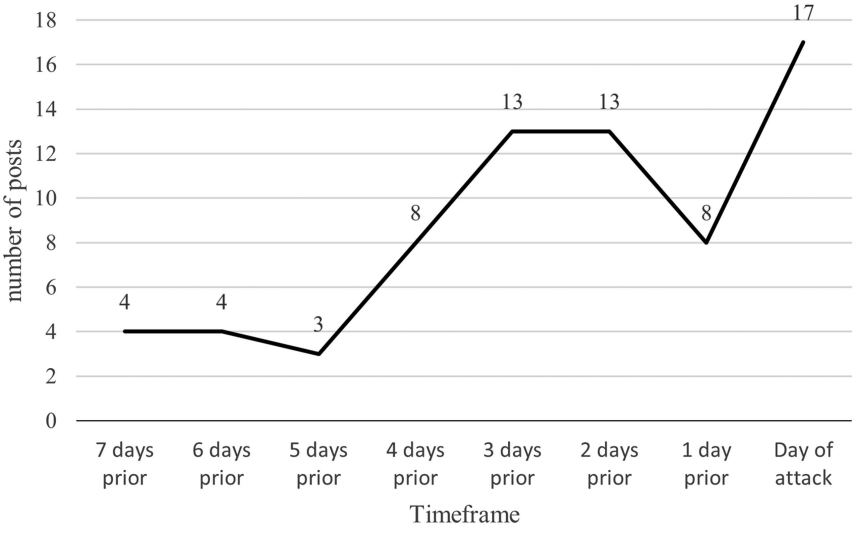


Figure 6
Graphic Revision of the Perpetrator Based on a Photo of the Perpetrators of the Columbine High School Rampage (1999) After Their Suicides

Note. EGS = embers ghosts squad. See the online article for the color version of this figure.

crime approached. At the same time, he began a countdown to his "final production." The last resort warning behavior is fulfilled.

Direct Threat—Communication of a Direct Threat to the Target or Law Enforcement

Whether or not the perpetrator made death threats directly to his later victims remains unclear. However, he regularly flooded the online public with death threats. For example, on Twitter he wrote, "I won't stop until every human on Earth is killed" (November 3, 2016, 217 days before the attack) or "I'm gonna pull out a goddamn shotgun and blow your damn head off!!! Do you understand?! You little worthless piece of crap!" (July 19, 2016, 324 days before the attack). This is also a quote from a Columbine perpetrator.

In a Twitter post at the end of January 2017, he added the following text to an image file: "bitch I'll kill u" (January 22, 2016, 503 days before the attack). He may have been addressing a fangirl with whom he had gotten into an argument, about which he elaborates in his offline texts.

Elsewhere on Twitter, he published a drawing showing Alias 2 stabbing a girl with a knife (December 31, 2016, 159 days before the attack). In combination with the text, a direct death threat is made here: "Ohhh [name] … We could've been pals. … If only you weren't so fucking whory on your social media. … It was a passing thought, but FUCK YOU." One of his colleagues at the supermarket had the same first name. In a tweet in January 2017 (January 26, 2017, 133 days before the attack), he mentioned specific first names of people against whom he held fantasies of violence and even murder. The warning behavior directly communicated threat is fulfilled.

Discussion

The aim of the study was to describe warning behaviors in the digital sphere based on an individual case of a fame-seeking mass shooter in order to examine whether the data and self-revelations contained therein can be sufficient to determine risk for serious targeted violence. In the case presented here, the quality and quantity of the characteristics were sufficient to determine such a risk on the basis of the WBT. The management of cases or persons with high-risk potential for general security is an essential part of the law enforcement.

Figure 7
Last Twitter Post by the Perpetrator

Note. Photographed at the later crime scene. EGS = embers ghosts squad. See the online article for the color version of this figure.

In total, seven of the eight warning behaviors were fulfilled by the offender based on the publicly visible online behavior. Novel aggression alone was not recognizable on the basis of the material. In the following, we summarize the special features of a warning behavior analysis based on online information:

- During the pathway warning behavior, the perpetrator refrained from showing concrete acts of crime planning and only reported on his weapon purchases. He seems to have strategically separated certain information and behaviors between his online profiles. Therefore, at the warning behaviors, identification and pathway only become visible to us by looking at all of his online activities.
- The severity of the fixation becomes clear, apparent when one takes his statements literally.
- Identification warning behavior shows how important it is to assess all of a person's profiles, as content may be toned down depending on the profile or only shown in smaller fringe communities. Qualitative observations can help to assess this by differentiating between pure interest in a topic, intensive engagement with it, and identification with previous attackers or assassins or to "identify oneself as an agent to advance a particular cause or belief system" (Meloy, Hoffmann, et al., 2021, p. 4), in which the perpetrators or actions are evaluated positively and the actions are justified.
- Novel aggression warning behavior in the sense of the typology was not apparent on the basis of the online behavior. It is possible that he showed novel aggression warning behavior in his environment, which we were unable to verify with our possibilities. In his diary, he reports having yelled at a colleague for the first time. This unprecedented verbal escalation could at least be considered as an initial indication of a possible further increase in aggressiveness but does not match the typology for physical

violence. Including an individual's close environment is immensely important in order to gain insights into observable behavior and behavior changes.

- With regard to the energy burst warning behavior, the period of time over which online activities increased in the investigated case is remarkable: Not only the number of Twitter postings increased but also the number of accounts and pseudonyms used by the later offender. We observe an increase in energy burst warning behavior over the months preceding the attack, as well as within the 7 days prior to the attack. We also compared our findings to those of Kupper and Meloy (2023), who identified a complete cessation of online posting activity, or "going dark," prior to the incident. In our case, we did not find a complete cessation but an obvious reduction in the number of posts 1 day prior to the crime as well, which could indicate that other activities take up the person's time, possibly due to immediate preparatory acts. On the day of the crime itself, the number of posts increases again, as he now publishes his "digital set" (see Table 1, including his offline diary) on Twitter. However, there are no "cutoff" values marking a concrete number that indicates a high risk, which is why patterns of warning behaviors should always be viewed as a whole against the background of the individual dynamics of individual cases.
- Leakage: The fact that his first leakage warning behaviors occurred almost 2 years before the crime shows that it is highly relevant to subject such communication to a qualitative assessment. O'Toole (1999) distinguished between low-, medium-, and high-level threats; Cornell et al. (2004) distinguished between transient and substantive threats. Among other things, the authors regard high specificity (in terms of information on time, location, victim selection, or methods of carrying out the crime), plausibility, and repetition as an indicator for higher risk.
- Last resort warning behavior becomes apparent online in the form of depression and suicidal tendencies. However, the associated imperative and specificity of time and action are emphasized in his last posts, the day-long countdown, his farewell video "Westborough High School Massacre," and the suicide tapes, especially shortly before the crime. In our view, depression and suicidality should be easy to grasp online, especially through text and sentiment analysis (cf. Allwinn & Böckler, 2021; Ji et al., 2018). The severity and urgency may only become clear shortly before the acts or through the perpetrators' private material, which he partially published only a few hours before the attack.
- Direct threats were visible online, as was leakage warning behavior. Assessment tools can also be used to specify the risk in more detail (Cornell et al., 2004; O'Toole, 1999; Van Brunt, 2015). In his diary, he mentions specific people, such as work colleagues, whom he wanted to kill. However, as far as we know, the entries only became known after his crime.

The WBT (Meloy et al., 2012) is an effective tool for individual online risk assessment with regard to serious targeted acts of violence. The WBT is only used if there are already abnormalities and a more in-depth risk assessment appears necessary for the person. The WBT is also part of the terrorist radicalization assessment protocol-18 (Meloy, 2018; Meloy & Gill, 2016) for the risk assessment of terrorist actors. It was validated on different data sets (Meloy, Hoffmann, et al., 2021). Case management is already recommended even in the presence of a single warning behavior. In our opinion, this applies in particular to proximal warning behaviors. Pathway and last resort and subsequently *identification*, *energy burst*, and *novel* aggression indicate an increased risk, whereas leakage gives rise to an initial suspicion, which yet requires further analyses (Böckler et al., 2020; Meloy, Hoffmann, et al., 2021). New physical violence (novel aggression), which is shown for the first time and cannot be classified as a pathway, casts a different light on future behavior and signals a willingness to use violence.

The limitations of the typology include, for example, the fact that WBT is better able to assess more proximate offenses than offenses that are further in the future. The high false-positive rate for leakage warning behavior (Meloy, Hoffmann, et al., 2021) or the variations in individual warning behaviors depending on which form of serious targeted violence is considered (e.g., intimate partner violence vs.

lone actor terrorists) are reasons why specific instruments are being used and/or developed for specific acts of interpersonal violence.

The presence of warning behavior does not mean that the person will necessarily commit an act of violence but that the probability may be increased. Police and intelligence services must first assess whether a person actually poses a high risk and intends to carry out a serious, targeted act of violence (warn), whether the person should continue to be monitored (watch), or whether it is a false alarm and the person poses no danger to third parties. However, as soon as one or more warning behaviors are present, practitioners and analysts recommend a more detailed analysis and at least observation of the person's behavior and communication (Meloy, Hoffmann, et al., 2021). The following case management can ultimately also mitigate the risk, which is why repeated assessments with change-sensitive instruments (i.e., they must incorporate dynamic risk factors) are required.

Limitations

To increase the reliability and validity of the assessment and the specification of case management, it is advisable to (a) apply multidisciplinary teams, (b) include further assessment instruments, and (c) consider protective factors that mitigate potential risk (Lösel et al., 2018). Further sources of information are then available to police and intelligence services to increase the density of information. In addition to the exemplary possibilities for prevention and police emergency response outlined in the individual risk assessment approach, we are also aware of its limitations, such as the lack of direct contact with the individual and thus distant profiling, the limited timeliness and holistic case study of observed communication and behavior on the internet, and the sometimes highly dynamic nature of biographical and radicalization trajectories (which is why dynamic rather than static risk analysis tools should also be part of the assessment; see Kemmesies, 2022, for a critical discussion). For this reason, we do not speak of a prognosis and do not provide a point forecast with supposedly precise statistical parameters but rather refer to a risk assessment.

The case in question cannot be extrapolated and applied to other cases, but it does allow important insights that can hardly be presented on a quantitative level. The long start-up phase, the offender's diverse products, and his behavior in the digital public sphere offered many opportunities to show many facets of warning behavior.

Our study was made to explore the realm of feasibility. Although we did not examine the chronology of the warning behaviors in depth, the sequence in the present case seems to be comparable to the outcomes of other studies on this specific question by Meloy, Goodwill, et al. (2021) and Ahlig et al. (2024). In particular, fixation and identification warning behavior are already shown with more temporal distance to the action, whereupon directly communicated threat, last resort, pathway, and energy burst warning behaviors follow at a later point in time and are therefore closer to the action. This issue was not considered as part of our feasibility study due to the specific subject matter but should be addressed in further research that also deals specifically with the transfer of such findings to the operational area. In a next step, it would be useful to have several experts code online postings by perpetrators and by people from their relevant networks who later did not become perpetrators, which would allow for discriminant validation and intercoder reliability testing.

Conclusions

The analysis of online communication is a promising approach when it comes to recognizing the potential danger of serious, targeted violence in the run-up to a crime. In our opinion, the perpetrator's internet communication, in particular the photo and video material uploaded by him, contained some starting points that, depending on legal regulations, would have made it possible to identify the perpetrator or the subsequent crime scene or at least to narrow down the area. For example, he showed photos of a specific playground, several portrait shots of himself, as well as a picture in a hospital in which he can be seen with two bandaged arms in a hospital gown with a recognizable logo. A video on YouTube shows his former school. Even his legal name is included in the credits of another video.

However, the large volume of information that floods the digital space on a daily basis cannot be easily managed by employees of police and intelligence services. For example, artificial intelligence-based linguistic tools could be used to analyze a person's mental and emotional states, the content of concrete statements could be

condensed, and image and video material could be analyzed to gain information on temporal and spatial context. Furthermore, individual features of the case could be compared with other cases by machine. This could provide a qualitative assessment of the further course of events in the form of possible scenarios, for instance, which actions by the perpetrator are to be expected in what period. The output could also inform about which information to look for to increase the validity of the prognosis. It could also give a recommendation in order to create a basis for further police action, with operational decisions to be taken by experienced professionals. As the decisions can have far-reaching consequences under certain circumstances, the (partially) automated evaluation requires critical monitoring, constant analysis of possible bias, further development, and evaluation.

References

Ahlig, N., Allwinn, M., Leuschner, V., Allely, C., & Scheithauer, H. (2024). *Perceived proximal warning behaviors in cases of severe targeted violence at German schools: A retrospective longitudinal analysis* [Manuscript submitted for publication]. Department of Education and Psychology, Freie Universität Berlin.

Allwinn, M., & Böckler, N. (2021). Crawling in the dark—Perspectives on threat assessment in the virtual sphere. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (2nd ed., pp. 283–300). Oxford University Press.

Allwinn, M., Hoffmann, J., & Meloy, J. R. (2019). German mass murderers and their proximal warning behaviors. *Journal of Threat Assessment and Management*, *6*(1), 1–22. https://doi.org/10.1037/tam0000122

Allwinn, M., Tultschinetski, S., & Görgen, T. (2022). Blazing hate into the world: Psychological case study of a fame-seeking rampage shooter. *Violence and Gender*, *9*(1), 42–56. https://doi.org/10.1089/vio.2021.0037

Altmeyer, M. (2019). *Ich werde gesehen, also bin ich: Psychoanalyse und die neuen Medien* [I am seen, therefore I am: Psychoanalysis and the new media]. Vandenhoeck & Ruprecht.

Berger, J. M. (2016). *The Turner legacy: The storied origins and enduring impact of White nationalism's deadly bible*. Terrorism and Counter-Terrorism Studies. https://doi.org/10.19165/2016.1.11

Böckler, N., Allwinn, M., Metwaly, C., Wypych, B., Hoffmann, J., & Zick, A. (2020). Islamist terrorists in Germany and their warning behaviors: A comparative assessment of attackers and other convicts using the TRAP-18. *Journal of Threat Assessment and Management*, *7*(3–4), 157–172. https://doi.org/10.1037/tam0000150

Calhoun, F., & Weston, S. (2015). Perspectives on threat management. *Journal of Threat Assessment and Management*, *2*(3–4), 258–267. https://doi.org/10.1037/tam0000056

Collins, R. (2014). Micro-sociology of mass rampage killings. *Revue de Synthese*, *135*(4), 405–420. https://doi.org/10.1007/s11873-014-0250-2

Cornell, D. G., Sheras, P. L., Kaplan, S., McConville, D., Douglass, J., Elkon, A., McKnight, L., Branson, C., & Cole, J. (2004). Guidelines for student threat assessment: Field-test findings. *School Psychology Review*, *33*(4), 527–546. https://doi.org/10.1080/02796015.2004.12086266

Federal Criminal Police Office, Federal Office for the Protection of the Constitution, & Hesse Information and Competence Centre Against Extremism. (2017). *Analysis of the background and process of radicalization among persons who left Germany to travel to Syria or Iraq based on Islamist motivations*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2017AnalysisOfTheBackgroundAndProcessOfRadicalization.pdf?__blob=publicationFile&v=2

Gill, P., Silver, J., Horgan, J., & Corner, E. (2017). Shooting alone: The pre-attack experiences and behaviors of U.S. solo mass murderers. *Journal of Forensic Sciences*, *62*(3), 710–714. https://doi.org/10.1111/1556-4029.13330

Helfgott, J. B. (2015). Criminal behavior and the copycat effect: Literature review and theoretical framework for empirical investigation. *Aggression and Violent Behavior*, *22*, 46–64. https://doi.org/10.1016/j.avb.2015.02.002

Hoffmann, J., & Allwinn, M. (2016). Amokläufe an Schulen durch Außenstehende—Psychiatrische Auffälligkeiten und Risikomarker [School shootings by outsiders—Psychiatric abnormalities and risk markers]. *Zeitschrift für Kinder- und Jugendpsychiatrie und Psychotherapie*, *44*(3), 189–197. https://doi.org/10.1024/1422-4917/a000421

Hoffmann, J., Meloy, J. R., Guldimann, A., & Ermer, A. (2011). Attacks on German public figures, 1968–2004: Warning behaviors, potentially lethal and non-lethal acts, psychiatric status, and motivations. *Behavioral Sciences & the Law*, *29*(2), 155–179. https://doi.org/10.1002/bsl.979

Janak, E., & Pescara-Kovach, L. (2017). Four decades, three songs, too much violence: Using popular culture media analysis to prepare preservice teachers for dealing with school violence. *Dialogue: The Interdisciplinary Journal of Popular Culture and Pedagogy*, *4*(1), 50–63. http://journaldialogue.org/issues/v4-issue-1/four-decades-three-songs-too-much-violence-using-popular-culture-media-analysis-to-prepare-preservice-teachers-for-dealing-with-school-violence/

Ji, S., Yu, C., Fung, S., Pan, S., & Long, G. (2018). Supervised learning for suicidal ideation detection in online user content. *Complexity*, *2018*(1), Article 6157249. https://doi.org/10.1155/2018/6157249

Kemmesies, U. E. (2022). Prognosefähigkeit: Herausforderungen zur Prognose von Radikalisierung und Terrorismus [Predictive ability: Challenges in predicting radicalization and terrorism]. In L. Rothenberger, J. Krause, J. Jost, & K. Frankenthal (Eds.), *Terrorismusforschung: Interdisziplinäres Handbuch für Wissenschaft und Praxis* [Terrorism research: Interdisciplinary handbook for science and practice] (Vol. 3, pp. 781–794). Nomos Verlagsgesellschaft. https://doi.org/10.5771/9783748904212

Kupper, J., & Meloy, J. R. (2021). TRAP-18 indicators validated through the forensic linguistic analysis of targeted violence manifestos. *Journal of Threat Assessment and Management*, *8*(4), 174–199. https://doi.org/10.1037/tam0000165

Kupper, J., & Meloy, J. R. (2023). *Going dark: The inverse relationship between online and on the ground pre-offense behavior in targeted attackers*. Global Network on Extremism and Technology. https://doi.org/10.18742/pub01-162

Lankford, A. (2016). Fame-seeking rampage shooters: Initial findings and empirical predictions. *Aggression and Violent Behavior*, *27*, 122–129. https://doi.org/10.1016/j.avb.2016.02.002

Lankford, A. (2018). Do the media unintentionally make mass killers into celebrities? An assessment of free advertising and earned media value. *Celebrity Studies*, *9*(3), 340–354. https://doi.org/10.1080/19392397.2017.1422984

Lankford, A., & Madfis, E. (2018). Don't name them, don't show them, but report everything else: A pragmatic proposal for denying mass killers the attention they seek and deterring future offenders. *American Behavioral Scientist*, *62*(2), 260–279. https://doi.org/10.1177/0002764217730854

Liem, M., van Buuren, G., & Schönberger, H. (2018, April 10). *Cut from the same cloth? Lone actor terrorists versus common homicide offenders*. International Centre for Counter-Terrorism. http://www.jstor.org/stable/resrep29424

Lösel, F., King, S., Bender, D., & Jugl, I. (2018). Protective factors against extremism and violent radicalization: A systematic review of research. *International Journal of Developmental Science*, *12*(1–2), 89–102. https://doi.org/10.3233/DEV-170241

Meloy, J. R. (2018). The operational development and empirical testing of the Terrorist Radicalization Assessment Protocol (TRAP-18). *Journal of Personality Assessment*, *100*(5), 483–492. https://doi.org/10.1080/00223891.2018.1481077

Meloy, J. R., & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, *3*(1), 37–52. https://doi.org/10.1037/tam0000061

Meloy, J. R., Goodwill, A., Clemmow, C., & Gill, P. (2021). Time sequencing the TRAP-18 indicators. *Journal of Threat Assessment and Management*, *8*(1–2), 1–19. https://doi.org/10.1037/tam0000157

Meloy, J. R., Hoffmann, J., Bibeau, L., & Guldimann, A. (2021). Warning behaviors. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (2nd ed., pp. 45–67). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0003

Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, *30*(3), 256–279. https://doi.org/10.1002/bsl.999

Meloy, J. R., Hoffmann, J., Roshdi, K., Glaz-Ocik, J., & Guldimann, A. (2014). Warning behaviors and their configurations across various domains of targeted violence. In J. R. Meloy & J. L. Hoffman (Eds.), *International handbook of threat assessment* (pp. 39–53). Oxford University Press.

Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law*, *29*(4), 513–527. https://doi.org/10.1002/bsl.986

Mohandie, K., & Duffy, J. E. (1999). First responder and negotiation guidelines with the paranoid schizophrenic subject. *FBI Law Enforcement Bulletin*, *68*, 8–16.

National Threat Assessment Center. (2020). *Mass attacks in public spaces—2019*. U.S. Secret Service, Department of Homeland Security. https://www.secretservice.gov/sites/default/files/reports/2020-09/MAPS2019.pdf

Nitsche, K., Allwinn, M., Hoffmann, J., & Bongard, S. (2020). Amokfahrten in Deutschland. Eine phänomenologische Annäherung und Untersuchung der Warnverhaltentypologie [Vehicle-ramming attacks in Germany. A phenomenological approach and examination of the warning behavior typology]. *Forum Kriminalprävention*, *2*, 22–26.

O'Toole, M. E. (1999). *The school shooter: A threat assessment perspective*. Critical Incident Response Group, FBI Academy, National Center for the Analysis of Violent Crime.

Richards, L., Molinaro, P., Wyman, J., & Craun, S. (2019). *Lone offender: A study of lone offender terrorism in the United States (1972–2015)*. U.S. Department of Justice, Federal Bureau of Investigation.

Robertz, F. J., & Kahr, R. (2016). Am Anfang war das Wort—Ein kommunikationswissenschaftlicher Blick auf Berichterstattung als Anlass zur Eskalation von Gewalt [In the beginning was the word: A communication studies perspective on the role of reporting in the escalation of violence].

F. J. Robertz & R. Kahr (Eds.), *Die mediale Inszenierung von Amok und Terrorismus: Zur medienpsychologischen Wirkung des Journalismus bei exzessiver Gewalt* (1st ed., pp. 13–27). Springer. https://doi.org/10.1007/978-3-658-12136-5_2

Shoemaker, P., & Cohen, A. (2005). *News around the world: Content, practitioners, and the public*. Routledge. https://doi.org/10.4324/9780203959091

Shrestha, A., Kaati, L., & Akrami, N. (2019). PRAT—A tool for assessing risk in written communication. *2019 IEEE International Conference on Big Data (Big Data)* (pp. 4755–4762). IEEE. https://doi.org/10.1109/BigData47090.2019.9006244

Silva, J. R., & Greene-Colozzi, E. A. (2021). Mass shootings and routine activities theory: The impact of motivation, target suitability, and capable guardianship on fatalities and injuries. *Victims & Offenders*, *16*(4), 565–586. https://doi.org/10.1080/15564886.2020.1823919

Silver, J., Horgan, J., & Gill, P. (2018). Foreshadowing targeted violence: Assessing leakage of intent by public mass murderers. *Aggression and Violent Behavior*, *38*, 94–100. https://doi.org/10.1016/j.avb.2017.12.002

Silver, J., & Silva, J. R. (2022). A sequence analysis of the behaviors and experiences of the deadliest public mass shooters. *Journal of Interpersonal Violence*, *37*(23–24), NP23468–NP23494. https://doi.org/10.1177/08862605221078818

Staudenmaier, P. (2021). The Unabomber manifesto in historical context. In P. Staudenmaier (Ed.), *Ecology contested: Environmental politics between left and right* (pp. 46–116). New Compass Press.

Surette, R. (2016). Measuring copycat crime. *Crime, Media, Culture*, *12*(1), 37–64. https://doi.org/10.1177/1741659015601172

Van Brunt, B. (2015). Violence Risk Assessment of the Written Word (VRAW2). *Journal of Campus Behavioral Intervention*, *3*, 12–25. https://doi.org/10.17732/JBIT2015/2

Van Brunt, B. (2016). Assessing threat in written communications, social media, and creative writing. *Violence and Gender*, *3*(2), 78–88. https://doi.org/10.1089/vio.2015.0050

Ware, J. (2020). *Testament to murder: The violent far-right's increasing use of terrorist manifestos* [ICCT policy brief]. International Centre for Counter-Terrorism.

Wertheimer, M. (1938). Gestalt theory. In W. D. Ellis (Ed.), *A source book of gestalt psychology* (pp. 1–11). Kegan Paul, Trench, Trubner. https://doi.org/10.1037/11496-001

Westermeyer, J. (1982). Amok. In C. T. H. Friedmann & R. A. Faguet (Eds.), *Extraordinary disorders of human behavior* (pp. 173–190). Springer. https://doi.org/10.1007/978-1-4615-9251-8_10

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. RAND Corporation. https://doi.org/10.7249/RR1964

Received February 11, 2024
Revision received August 3, 2024
Accepted September 22, 2024 ■