



Threat Assessment on College Campuses

9

Philip A. Saragoza, Stephen G. White, and Victor Hong

Introduction

The tragic shootings at Virginia Tech in 2007, and Northern Illinois University in 2008, marked a significant turning point in campus violence risk awareness. Campus shootings had occurred before, even prior to the 1966 University of Texas tower shootings. Prevention efforts began to appear in the late 1980s and continued to be established. The report from the Governor's Virginia Tech Review Panel, however, specifically spelled-out systemic issues for campuses, gaining the attention of administrators nationally. Hampered by confusion about privacy laws, the Virginia Tech student's "behaviors of concern" existed in information silos, while "passivity" characterized the school's response to these behaviors. Treatment resources were lacking. Significantly, no one on the university's Care Team had expertise in *threat assessment*: "No one connected all the dots" that the young man had the personal motives for an attack and was engaging in preparatory behaviors on a *pathway to targeted violence* – not impulsively, but a consciously planned act of predation, emotionless as he carried it out [1].

In a text devoted to campus mental health issues, however, we emphasize – in addressing the serious issue of violence on campus, mental illness per se is not the cause. Any attempt to identify a single factor as the main reason as to why individuals choose violence as a response to their circumstances is an oversimplification. Threat assessors do look for certain constellations of beliefs, behaviors, and contextual factors that fuel, enable, or signal attacks, but there is no useful, objective profile of a mass murderer [2–4].

P. A. Saragoza · V. Hong (✉)
Department of Psychiatry, University of Michigan, Ann Arbor, MI, USA
e-mail: vhong@med.umich.edu

S. G. White
Work Trauma Services, Inc., San Francisco, CA, USA
e-mail: swhite@wtsglobal.com

Although violence risk on campuses may be posed by employees, faculty, and outsiders as well, which threat assessment teams must contend with and address, the focus of this chapter will be on the student-of-concern. Risk factors will be noted and a prevention model outlined. Described is the practice of threat assessment in dynamic campus contexts: an information-driven, ongoing process to assess the risk, nature, and severity of violence posed by an individual, which informs decisions for risk mitigation actions and related interventions [2, 5, 6].

Background and Trends

In 2010, the US Department of Education, US Secret Service, and the FBI combined investigative resources, resulting in a widely recognized report, *Campus Attacks: Targeted Violence Affecting Institutions of Higher Education* [7]. In the period between 1900 and 2008, the authors identified 272 cases that met the inclusion criteria for targeted violence. Studied were directed assaults against specific or random targets, using lethal force or the ability for lethal force, and not limited to homicides. Nearly 60% of the incidents had occurred since 1990, and 45% of the perpetrators were current students, 15% former students. Among the findings were that in 31% of the cases the subject's pre-incident behaviors of concern were identified by outside observers (e.g., mental symptoms, suicidal ideas, nonspecific threats, increased isolation, interest in or acquisition of weapons). Ten percent had acted violently toward the victim prior to the incident, and 13% of subjects threatened victims verbally or in writing. In over 80% of cases, precipitating events (rejection, failure, or acute losses) were identifiable. In 75% of the cases, the subject had a specific target in mind. The most common motive was retribution in the context of a relationship (34%). Other motives included response to academic stress (10%), acquaintance or stranger sexual violence (10%), and workplace dismissal of staff (6%). Clearly, the "signs" are very often visible.

As stated by the US Secret Service behavioral scientists in their influential study of assassins and attackers of public figures, incidents of targeted violence are "the end result of an understandable and often discernable process of thinking and action" [8]. Targets may either be people personally known to the individual, symbolic (e.g., "socially successful students"), places, public figures, or a product of an attacker's delusions. Although the timeline may be quite variable in individual cases, pre-attack behaviors more or less follow an identifiable sequence. Therein lies the key to detection and possible prevention.

While most violent crime statistics have been gradually declining since the 1990s, the frequency of mass murders and attempted attacks in public places – schools, workplaces, houses of worship, entertainment and other venues – has markedly increased, casting a grim spectre over education and work life and social pastimes [9, 10]. Although causation cannot be assumed, paralleling this rise over the past 15 to 20 years is the growth of social media and its influence on beliefs and

behavior. Extremist digital communities encourage the disinhibition of hostility, expression of hate speech, and “toxic masculinity” [11, 12], and may contribute to violent motives [12–15].

Perpetrator Thinking and Behaviors on the Pathway to Violence

Violence risk is complex but comprehensible. An individual’s pathway to targeted violence typically begins with a *grievance* – real, exaggerated, or imagined [5, 6]. Grievances in these instances are beyond the magnitude and meaning experienced by anyone and everyone in the course of life but that do not lead to violence as a “remedy.” Grievances contributing to risk are typically rooted in profound feelings of injustice over perceived wrongs, and include four elements: loss, humiliation, anger, and blame (J.R. Meloy, Expert in forensic psychology. Personal communication, Feb 2020). *Violent ideation* and fantasies follow, and are ego-syntonic and boosting of self-esteem. On college campuses, teams may see a wide range of grievances in persons of concern, including rejection by intimate partners or the thwarting of romantic interests, or anger toward faculty over academic troubles (especially if driven by family or cultural pressure to achieve). Of concern as well are paranoid thinking or delusions with violent content, fixations, and stalking [16]. A sequence of decisions, potentially detectable in communications or behavior, will typically unfold: the grievant believes that violence is justified, and has rejected sanctioned methods for resolution such as judicial remedies, seeking professional help, or just “letting it go” [17]. The individual has determined the means for violence, and – in varying degrees of detail, will more or less engage in *research and planning* for the attack, further *pre-attack preparation*, perhaps *probing and breaches* at the chosen site, culminating in the *attack* itself. The pathway model is illustrated in Fig. 9.1.

Of great importance is the mass attacker’s decision to willingly pay the price – death or imprisonment – for their actions. Between a third to one-half of those who commit mass murder on campus or in other public venues either die by suicide, provoke a “suicide-by-cop”, or will surrender without resistance [18]. Assessing suicide risk along with risk to others is essential, then, as the pathway is by nature a “nothing to lose” self-destructive journey, but not before staging a dramatic, omnipotent spectacle of violence toward others. A number of attackers, often socially marginalized and seeing no future, have left manifestos or otherwise communicated that the violence was embraced as an *accomplishment*, making their life “worth something,” at last. To paraphrase psychiatrist and researcher James Gilligan, violence is often an attempt to replace feelings of shame with feelings of pride [19]. The notoriety and infamy achieved by the shooter, aware of the “cultural script” assuring he will live on – on the internet after his death, is an example of the profoundly troublesome side effects of our digital age [20].

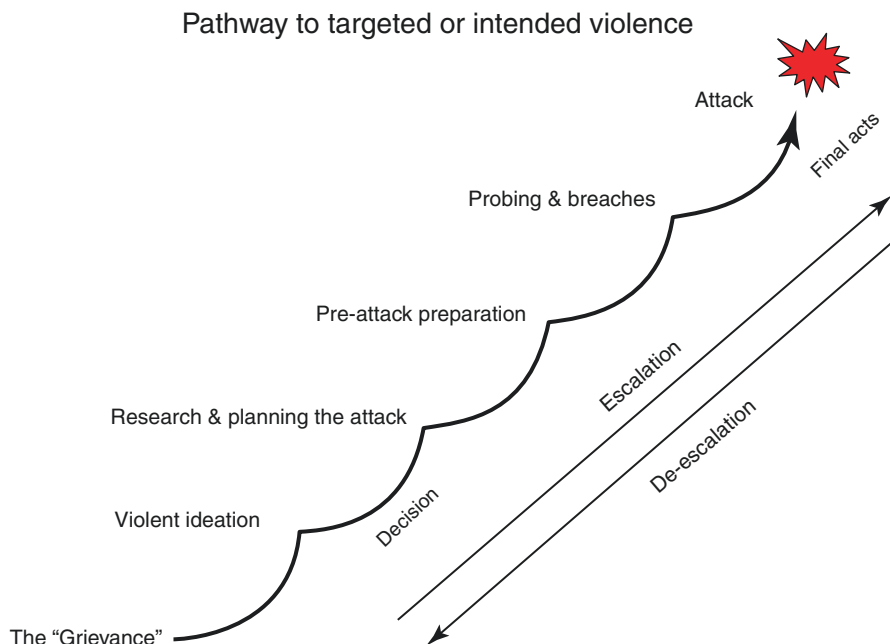


Fig. 9.1 Pathway graphic. (Adapted with permission from Calhoun and Weston [5] © 2003. All rights reserved. Adapted by White and Meloy [16])

Prevention and Best Practices

From various reviews, analyses and accumulated case experience, a *standard of care* has emerged for campus violence prevention [21]. Legislation is following. In 2013, the State of Virginia mandated the development of threat assessment plans for their public colleges and universities (Code of Virginia § 23.1–805). A report from the U.S. Department of Justice regarding threat assessments stated:

... violence prevention... cannot be a passive process. It requires a strong and overt commitment by organizations and communities to prioritizing public safety and caretaking for those in need. This is manifested by adoption of policies and programs to support targeted violence prevention efforts, establishment of threat assessment and management teams, and education to underscore the importance of these processes and to promote acceptance and engagement by all [22].

At the heart of protocols is the multidisciplinary threat assessment team, comprised of professionals from different campus departments who bring their expertise, perspective, and guidance to bear on the task. Typical members include representatives from the department of public safety, student judicial affairs, residential life, human resources, campus counsel, the counseling or mental health center, and others, depending on the size, structure, and nature of the institution.

Desirable individual attributes include a passion for the work, sufficient personal resilience, a collaborative work style, and knowledge of the institution's processes, culture, and politics.

Most teams are advisory to decision-makers but must avoid the error of being “a team in name only.” Deisinger, Randazzo, and Nolan [21] state that a team can only be effective when it facilitates a process that does the following:

- (1) enables centralized awareness of developing concerns through an active outreach program,
- (2) conducts a thorough and contextual assessment of the situation,
- (3) implements proactive and integrated case management plans,
- (4) monitors and reassesses the situation on a longitudinal basis,
- (5) staffs the process with an effective and relevant multidisciplinary team, and
- (6) conducts all these practices in accordance with relevant laws, policies, and standards.

To not have the proper ingredients in place is to invite potential chaos, as *any* case, regardless of what, objectively at least, its real potential risk may be, can very quickly create significant fear and disruption. Affected members of the campus community expect management to respond competently and confidently. Unaddressed fear or reactive, ill-informed responses result in anger and lack of trust.

Two important elements are (1) that all team members receive basic training (and continuing education) in the principles of threat assessment, the risk factors for violence, and the nature of case management dynamics in “live” organizational contexts; and (2) that they have threat assessment experts available to confer with when prudent.

Inherent and conflicting legal obligations abound. The team's attorney is in the role of identifying and balancing common exposures and informing others of the possible legal implications of various considered actions. Besides the obvious obligations to potential targets are those to any student of concern. Liability stems from a variety of legal theories, including occupational health and safety statutes, privacy, discrimination including Americans with Disabilities Act, wrongful death, due diligence, and a duty to warn and protect, among others. Refer to other sources for in-depth discussion of these issues [23].

That many attacks are susceptible to detection is not the same as presuming to predict violence, which is impossible. It is more accurate to depict threat assessment practice as a *protective investigation*, intended to “identify and manage behaviors of concern in the present” (J.R. Meloy, Expert in forensic psychology. Personal communication, Oct 2019). Relying on evidence-based, rational, and relatively transparent risk (and protective) factor indicators, the process is more defensible. Protective investigations are not adversarial in nature, especially in campus contexts, and are not the same as misconduct or criminal investigations. The databases for these three endeavors may overlap, and may run parallel in time. Their goals, however, differ, as do the obligations of those conducting them. In essence, safety trumps other concerns, and discipline for threats in the absence of a careful assessment may result in unintended consequences, a process issue that teams and other stakeholders need to be cognizant of.

Late adolescence and early adulthood being the time when major mental disorders are often first manifest, institutions of higher learning espouse more of a

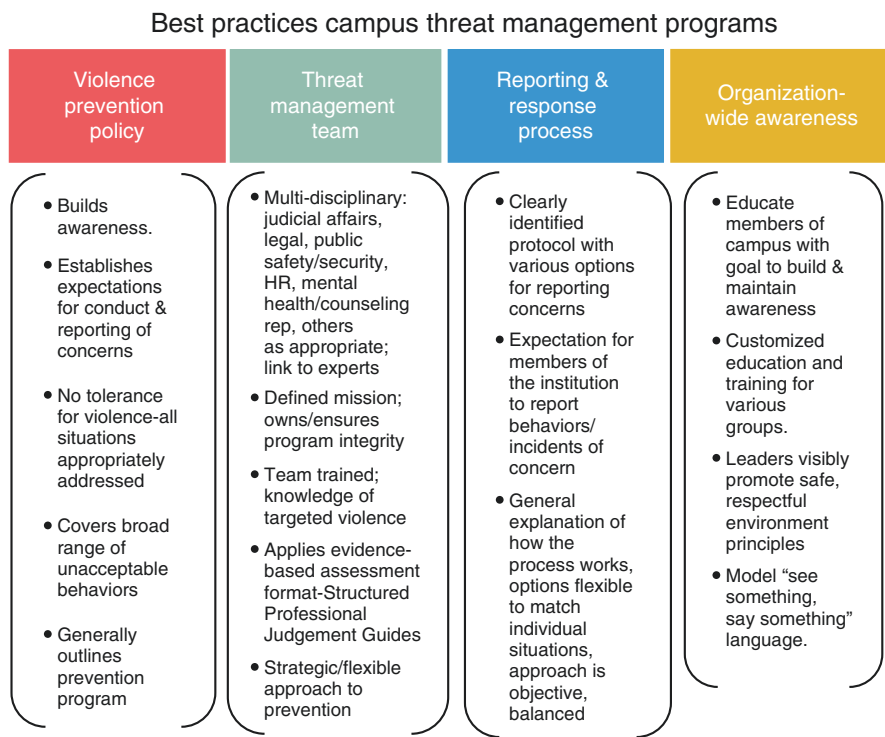


Fig. 9.2 Best practices graphic. (© 2020. Stephen G. White. All rights reserved)

rehabilitative philosophy toward the troubled but troubling student whenever possible. Many such students, including those who raise concern, may be offered treatment, leaves of absence, and other interventions intended to help them, as well as to mitigate any risk. Figure 9.2 shows a graphic of best practices in campus settings.

Steps in Case Assessment and Management

Threat management often requires striking the right balance between a need for speed and for adequate information. The standard of care strives for assessments being thorough, fair, accurate, and objective. Multiple avenues for reporting concerns, including an anonymous option, must be available and known to members of the campus community. Separating assessment from case management is somewhat arbitrary. The two are intertwined – screening informing initial actions, leading to new data that informs decisions for the next actions steps, leading to yet more data on how the individual is responding, etc.

Screen initial reports. Incident reports or expressed concerns may come from various sources, and vary widely in their nature and apparent seriousness. If any of the

following five indicators are present, further inquiry should follow: threats or expressed ideas to harm self or others; bizarre thinking or irrational suspiciousness unsupported by facts (especially if they include any violent content); circumstances, losses, or anticipated events that might affect the likelihood of violence; the individual identified as troubled has access to weapons or is attempting to gain access; or involved or reporting parties are otherwise concerned about possible violence to self or others [16].

In practice, many individuals who make a threat or reveal any of the recognized pre-incident behaviors do not actually pose a threat [8]. A large proportion of the cases presented to a team are false positives – the individual has no violent intent. Efficiencies are needed in triaging cases so as not to over-react to “unsubstantial” threats or situations. In large institutions at least, teams are compelled to develop the internal skills and experience to work through the “haystack” of reports, so as to identify any “substantial” scenarios, and to redirect other matters, once screened, to appropriate resources. All incident reports, however, need to be adequately investigated. An everyday mantra should be, “when in doubt, confer.”

Conduct a threat assessment inquiry. Assessment involves comprehensive and ongoing fact-finding. Data sources include records, collateral interviews, social media posts, and often engagement with the individual of concern, almost always if he or she is a current student. The goal of campus risk assessment interviews, whether conducted by mental health professionals or skilled non-clinicians, is to understand the individual and his or her thoughts, feelings, possible motives, or any mental symptoms suggesting a risk of harm. The purpose is not to elicit confessions or otherwise strip the interviewee psychologically bare. The strategy is to listen, and to identify to the degree possible any actual momentum toward the choice of violence versus foregoing destruction of self and others. Concerning behaviors are absolutely addressed, as well as probing for what events or actions could exacerbate risk, and what actions or interventions could mitigate risk. Various resources discuss interview strategies in more detail [e.g., 16, 24].

A growing trend is the development and use of structured professional judgment guides (SPJs). These assessment instruments are intended to reflect the state of the discipline, based on empirical knowledge of risk and protective factors and professional practice. An SPJ identifies a set of risk factors to consider in evaluations of certain populations of concern, e.g., The Stalking Risk Profile (SRP), the Risk for Sexual Violence Protocol (RSVP), the HCR-20 – often used to assess the risk posed by violent prisoners being considered for release – the Spousal Assault Risk Assessment (SARA), and the Terrorist Radicalization Assessment Protocol (TRAP-18). The WAVR-21 V3 is an SPJ designed for the assessment of workplace and campus targeted violence, and can also be supplemented with other SPJs such as mentioned above [16].¹ SPJs improve the consistency, transparency, and appropriateness of case management decision-making. They are not actuarial tools, and they are not a substitute for assessors’ clinical or professional judgment.

¹ Author White acknowledges a commercial interest in the WAVR-21.

Assessors must weigh and integrate the factors present in a case, and the pros and cons of various intervention options. As stated by Monahan and his colleagues in the MacArthur study of mental disorder and violence – when assessing risk, “...clinical judgment – aided by an empirical understanding of risk factors for violence and their interactions – reflects, and in our view should reflect, the standard at this juncture in the field’s development” [25].

Consider intervention options. A variety of intervention options are possible, and vary from “soft” and supportive to “hard” – prosecution and imprisonment. No one size fits all. Judgment is always needed and strategies can change.

Deisinger et al. propose a systemized approach for assessment and management that reflects the contextual and dynamic nature of targeted violence, abbreviated as “STEP” to represent the four domains for consideration [21]. These include assessment of the *Subject* (the behaviors, traits, characteristics and history of the individual of concern that suggest risk); *Target* (their physical vulnerability); *Environment* (how contextual factors or systems facilitate or enable violence); and *Precipitating event* (occurrences or decisions that may trigger escalations of concerning behavior). Viable management strategies or options are then considered that address the four domains: *Subject* (e.g., de-escalate, contain, control, attempt to help the individual of concern, or facilitate an involuntary hospitalization); *Target* (decrease their vulnerabilities through heightened protection or target hardening); *Environment* (modify physical environments to discourage violence or intercept any problematic approaches); and *Precipitating event* (prepare for and/or mitigate precipitating events that could trigger adverse reactions).

Over-arching assessment questions to guide targeted violence risk inquiries in organizational settings have been proposed by various authors. The following is a list of ten key investigative questions largely drawn from those first proposed by the US Secret Service and later modified slightly by Deisinger, Randazzo, and Nolan, as well as by White and Meloy [8, 16, 21].

1. What are the subject’s behaviors, or the conditions, that brought him or her to attention, and is there a discernable motive or explanation for his or her behaviors of concern?
2. Have there been any communications of any nature suggesting ideas, justification, or intent to attack others, or otherwise indicating the subject’s intentions?
3. Has the subject shown an inappropriate interest in or fixation on any of these topics: campus/workplace/school attacks or attackers; weapons; mass violence or terrorism; obsessive pursuit or stalking?
4. Has the subject engaged in any attack-related behaviors, such as developing a plan, approaching targets, assaults or attempted assaults, attempts to circumvent security, or menacing behavior or stalking?
5. Is the subject experiencing acute mental symptoms such as command hallucinations, delusional ideas or paranoia, with any violent content and/or accompanied by anger, and is there any indication of ever having acted on such beliefs?

6. Does the subject have the capacity and means to carry out an act of targeted violence?
7. Is the subject experiencing hopelessness, desperation, or despair, a recent loss in work, love, status, or financial stability, increasing isolation, or ever been suicidal?
8. Is the subject's conversation or "story" consistent with his or her actions?
9. Are other people, especially those who know the subject, concerned about his or her potential for violence?
10. What factors in the subject's life or environment might increase the likelihood of an attempted attack, or decrease the likelihood of an attempted attack?

Ways to Improve

While the number of campus threat assessment teams is increasing, widely variable practices exist, and standardization remains an aspirational goal. A common problem with campus programs is that threat assessment team membership is an additional obligation that its members – invariably busy administrators who are susceptible to distraction – are expected to take on. Program directorship should be recognized as a full-time position, adequately funded, with the duty to maintain best practices and program integrity. Sufficient training for team members and access to outside experts is a related issue. The broader use of structured risk assessment guides would improve the objectivity of assessors and make protocols more defensible.

Conclusion

Campuses are generally very safe places, but no institution is immune from violence, including the possibility of mass attacks. A great deal has been learned about the precursors to targeted violence, environmental and contextual enablers of violence, and the elements of effective protocols for prevention. Leadership needs to demonstrate a strong commitment to establishing and maintaining best practices and understand that, "A good place to study and work starts with a safe place to study and work."

Key Points

- Individuals on a pathway to violence typically engage in a sequence of thinking and behavior that is possible to detect and thwart.
- Most individuals who demonstrate risk-concerning behavior do not pose a risk, and many students of concern can be helped; all situations must be properly screened or assessed, and interventions and remedies individualized.

- Proactive campus prevention programs staffed by a multidisciplinary team with demonstrated competence in threat assessment is a best practice and increasingly the standard of care.

References

1. Virginia Tech Review Panel. Mass shootings at Virginia Tech, April 16, 2007: Report of the review panel presented to Governor Kaine, Commonwealth of Virginia. Richmond; 2007. p. 2.
2. Borum R, Fei R, Vossekuil B, Bergland J. Threat assessment: defining an approach for evaluating risk of targeted violence. *Behav Sci Law*. 1999;17:327–37.
3. Schouten R. Workplace violence and the clinician. In: Simon RI, Tardiff K, editors. *Violence assessment and management*. Washington, DC: American Psychiatric Publishing; 2008. p. 501–20.
4. Turner JT, Gelles MG. *Threat assessment: a risk management approach*. New York: Haworth Press; 2003.
5. Calhoun FS, Weston SW. *Contemporary threat management: a practical guide for identifying, assessing, and managing individuals of violent intent*. San Diego: Specialized Training Services; 2003.
6. Meloy JR, Hart SD, Hoffmann J. Threat assessment and threat management. In: Meloy JR, Hoffmann J, editors. *International handbook of threat assessment*. New York: Oxford University Press; 2014. p. 3–17.
7. Drysdale D, Modzeleski W, Simons A. *Campus attacks: targeted violence affecting institutions of higher education*. Washington, DC: U.S. Secret Service, U.S. Department of Education, and Federal Bureau of Investigation; 2010.
8. Fein R, Vossekuil B. Assassination in the United States: an operational study of recent assassins, attackers, and near-lethal approachers. *J Forensic Sci*. 1999;44:321–33.
9. Blair JP, Schweit KW. *A study of active shooter incidents in the United States between 2000 and 2013*. Washington, DC: Texas State University and Federal Bureau of Investigation; 2010.
10. Cohen AP, Azrael D, Miller M. Rate of mass shootings has tripled since 2011, Harvard research shows. 2014. <http://www.motherjones.com/politics/2014/10/mass-shootings-increasing-harvard-research>. Accessed 25 June 2020.
11. Blommaert J. Online-offline modes of identity and community: Elliot Rodger's twisted world of masculine victimhood. 2017. *Tilburg Papers in Culture Studies* 200. <https://biblio.ugent.be/publication/8551305/file/8551306.pdf>. Accessed 25 June 2020.
12. Jaki S, De Smedt T, Gwóźdz M, Panchal R, Rossa A, De Pauw G. Online hatred of women in the incels.me forum: linguistic analysis and automatic detection. *J Lang Aggress Confl*. 2019;7(2):240–68. <https://doi.org/10.1075/jlac.00026.jak>
13. Aiken M. *The cyber effect*. London: John Murray; 2016.
14. Colleoni E, Alessandro R, Arvidsson A. Echo chamber or public sphere?: predicting political orientation and measuring political homophily in Twitter using big data. *J Commun*. 2014;64(2):317–32. <https://doi.org/10.1111/jcom.12084.sd>.
15. Suler J. The online disinhibition effect. *Cyber Psychol Behav*. 2004;7(3):321–6. <https://doi.org/10.1089/1094931041291295>.
16. White SG, Meloy JR. *The WAVR-21: workplace assessment of violence risk: a structured professional judgment guide for the workplace assessment of violence risk, including campus and student contexts*. 3rd ed. San Diego: Specialized Training Services; 2016.
17. Hart SD, Logan C. Formulation of violence risk using evidence-based assessments: the structured professional judgment approach. In: Sturmey P, McMurrin M, editors. *Forensic case formulation*. Chichester: Wiley-Blackwell; 2011. p. 83–106.

18. Alathari L, Blair A, Carlock A, Driscoll S, Drysdale D, McGarry J. Mass attacks in public spaces – 2018. 2019. https://www.secretsservice.gov/data/press/reports/USSS_FY2019_MAPS.pdf. Accessed 25 June 2020.
19. Gilligan J. Shame, guilt, and violence. *Soc Res.* 2003;70(4):1149–80.
20. Newman KS, Fox C, Harding DJ, Mehta J, Roth W. *Rampage: the social roots of school shootings*. New York: Basic Books; 2004.
21. Deisinger ERD, Randazzo M, Nolan J. Threat assessment and management in higher education: enhancing the standard of care in the academy. In: Meloy JR, Hoffmann J, editors. *International handbook of threat assessment*. New York: Oxford University Press; 2014. p. 107.
22. Behavioral Analysis Unit. *Making prevention a reality: identifying, assessing, and managing the threat of targeted attacks*. United States Federal Bureau of Investigation; 2017.
23. Lies IIMA, Powers JJ. Employer liability and workplace violence. In: Lies IIMA, editor. *Preventing and managing workplace violence: legal and strategic guidelines*. Chicago: American Bar Association; 2008. p. 258–89.
24. Van der Meer BB, Diekhuis ML. Collecting and assessing information for threat assessment. In: Meloy JR, Hoffmann J, editors. *International handbook of threat assessment*. New York: Oxford University Press; 2014. p. 54–66.
25. Monahan J, Steadman HJ, Silver E, Appelbaum PS, Robbins PC, Mulvey EP, et al. *Rethinking risk assessment: the MacArthur study of mental disorder and violence*. New York: Oxford University Press; 2001. p. 134–5.