A Directory of Threat Assessment Models

Authors: Amber Seaward, Zoe Marchment, Paul Gill

UCL

NCITE NATIONAL COUNTERTERRORISM, INNOVATION, TECHNOLOGY, AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

About NCITE. The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security (DHS) Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science and Technology Office of University Programs, NCITE is the trusted DHS academic consortium of over 60 researchers across 18 universities and non-government organizations. Headquartered at the University of Nebraska at Omaha, NCITE is a leading U.S. academic partner for counterterrorism research, technology, and workforce development.

Acknowledgement. The research in this report was conducted in support of Award no. 70RSAT21G00000002, "Public Safety and Violence Prevention Evaluations," from the Department of Homeland Security (DHS) Science and Technology Directorate under Basic Ordering Agreement 70RSAT21FR0000084.

Disclaimer. Any opinions or conclusions contained herein are those of the authors and do not necessarily reflect those of the Department of Homeland Security, the DHS Science and Technology Directorate, or the University of Nebraska System.

Executive Summary

- Threat assessment is a process of identifying, assessing, and managing threats of targeted violence prompted by warning behaviours.
- Threat assessment is an evolving field with no singular guidebook that can cover the range of settings to which it is applied.
- Therefore, there are many different practical models of threat assessment implementation.
- This directory reviews how threat assessment is practically implemented in various settings, by systematically reviewing case study literature that describes the structure and operations of existing threat assessment teams and models.
- The directory compiles information on 27 threat assessment models which cover a range of harms within educational settings and workplaces as well as more specific crime types such as fixated threats to public figures, violent extremism, and stalking.
- For each of the 27 models, the directory outlines details about their background, team details and composition, the nature and structure of their referral system, their threat assessment operations, their case management structure, and their quality assurance processes.
- This directory serves as the foundation for a comparative analysis of threat assessment models with a focus on learning from partner countries outside of the United States.

Introduction

Threat assessment is a process of identifying, assessing, and managing threats of targeted violence prompted by warning behaviours (Harris & Lurigio, 2012; Meloy et al., 2021; Randazzo & Cameron, 2012). It was initially developed as a model by the United States Secret Service as a measure to prevent assassinations (Borum et al., 1999; Cornell & Burnette, 2021; Randazzo & Cameron, 2012), but has since emerged as a violence prevention measure in many settings, including workplaces, schools, universities, and general communities, within and outside the United States (Randazzo & Cameron, 2012).

The threat assessment approach grew in support following the Exceptional Case Study Project (Fein & Vossekuil, 1997) and Safe School Initiative (Vossekuil et al., 2004). These two studies analysed the personal histories and pre-incident behaviours of perpetrators of public figure attacks and targeted school violence respectively. Both studies found perpetrators tended to leak their intentions beforehand (though rarely with explicit threats), engage in planning on a path towards violence, suffer from personal grievances or losses, and not fit into a discernible profile of an attacker (Fein & Vossekuil, 1997; Vossekuil et al., 2015). Similar findings were replicated in numerous other studies and contexts, primarily concerning the prevalence of leakage (Meloy & O'Toole, 2011). These studies have informed general principles of threat assessment; attacks may be preventable, as there are opportunities for early identification and intervention to treat problems and manage risk (Fein & Vossekuil, 1997; Vossekuil et al., 2004).

The threat assessment model distinguishes itself from previously prominent violence prevention approaches: violence risk assessment, profiling, and reactive policing.

Contrary to violence risk assessment that is part of a scheduled process in law enforcement, judicial, or mental health decisions, the threat assessment process is initiated by a threat or other concerning behaviour (Borum et al., 1999; Lloyd, 2021; Meloy et al., 2012; 2021). It involves more dynamic, short term, and time sensitive situations with more limited information than scheduled risk assessment (Meloy et al., 2021; Mitchell & Palk, 2016; Van der Meer & Diekhuis, 2013). The focus is on more situational factors and current psychological symptoms than dispositional factors, historic diagnoses, or membership of empirical categories (Meloy et al., 2012; 2021). It tends to involve a particular target, rather than being part of a standardised process of managing a particular perpetrator (Meloy et al., 2021; Mitchell & Palk, 2016). Finally, threat assessment is carried out in a much wider range of operational settings, including private corporations (Meloy et al., 2021).

Contrary to profiling, threat assessment is focused on behaviours and motivations, rather than static characteristics and diagnoses (Borum et al., 1999; Randazzo & Cameron, 2012). Due to the rarity of attacks and the lack of an existing 'profile' of attackers, inferring behaviour from common personal characteristics can be harmful (Borum et al., 1999; Cornell, 2020b; Reddy et al., 2001). The majority who fit a 'profile' will not commit an offence, and those outside the profile might be missed (Reddy et al., 2001). Therefore, threat assessment examines the escalation of behaviour over time and corroborates information from multiple sources to reach a level of concern (Reddy et al., 2001; Vossekuil et al., 2015).

Finally, threat assessment differs from the traditional operations of law enforcement in investigating threats after a violent offence has been committed (Borum et al., 1999). There are new elements of management and assessment skills that must be learned by law enforcement practitioners in the pre-crime space (Borum et al., 1999).

While threat assessment clearly diverges from these approaches, it is still an evolving field with no singular guidebook that can cover the range of settings to which it is applied. Some regions have unique ethical or legal restrictions; some settings involve adolescent populations requiring different approaches and objectives; and some agencies merely consult on external investigations. Therefore, there are many different practical models of threat assessment implementation. Each tends to have standardised procedures for how cases are identified, assessed, and managed (Randazzo & Cameron, 2012). This directory reviews how threat assessment is practically implemented in various settings, by systematically reviewing case study literature that describes the structure and operations of existing threat assessment teams and models. It is hoped this directory can serve as a reference guide in future development of threat assessment teams.

Dimensions of the structure and operations of existing threat assessment models

The following dimensions were chosen to be analysed for each threat assessment model or team: the setup, team details, referrals structure, threat assessment operations, interventions, case management structure, and quality assurance.

Threat assessment setup

Background and objectives: an descriptive overview of the model, its origins, and its main objectives. Objectives can vary between violence prevention and violence prediction (Meloy et al., 2021), and can incorporate objectives beyond violence reduction, including student wellbeing, student or employee retention, or zero-tolerance policies.

Threat: the specific threat(s) that the team targets.

Basic information: the model's country, setting, date of formation, remit, funding source, and physical team location.

Other involvements: explanation of anything beyond the primary remit of threat assessment, such as research or intelligence for major events.

Team details

Specialist vs. multidisciplinary: the extent to which the team is multidisciplinary, including whether multidisciplinary agencies are fully integrated or involved in a more consultative way. The best practice consensus is for multidisciplinary teams, to liaise with other agencies to identify threats, combine perspectives for assessment, and facilitate optimal intervention (Deisinger & Nolan, 2021; Meloy et al., 2021; O'toole, 2000; 2021; Randazzo & Cameron, 2012).

Team structure: details surrounding the structure of how the team works on cases and the frequency of team meetings. This includes whether the team owns the case or acts as a consulting entity in a wider investigative process.

Core team: disciplines represented in the core team and whether the team has a specified team leader. Disciplines tend to include law enforcement, mental health professionals, administrative staff, legal counsel, social workers, and other community agencies.

Additional part time or consulted disciplines: additional resources consulted beyond the core team.

Training: details of levels of training or prior experience necessary for team members.

Training evaluation: details on whether and how training is evaluated.

Referrals structure

Case generation

Threat identification: whether cases are picked up by referral only, or by more proactive efforts to identify threats, such as by manual or automatic online monitoring of communications (Allwinn & Böckler, 2021).

Referral communication systems: including referring agencies and referral mechanisms. Threats are more likely to be reported and identified if there is an existing system to facilitate it (White, 2021), but these systems can vary in user awareness, and format (e.g. phone, email, online system).

Contact with referring bodies

Nature of contact with referring bodies: details on information and guidance provided to referring bodies and communities including screening tools, designated contacts, and training on the threat assessment process, how to identify leakage, and how to refer.

Audit of referral mechanisms: any processes to evaluate the referral process.

Threat assessment operations

Threat assessment process: details and order of the steps in the process. The overall process for most models is to separate the majority of reported cases that are of low concern, from the few that might present a real or imminent risk of violence (White, 2021). Within this, the stages of triage, involvement of multiple teams, and measures to control for bias, differ between models.

Resources used in threat assessment: potentially including the threatening communication, open-source information, police and criminal records, healthcare information, and often electronic activity of the subject (Allwinn & Böckler, 2021; Scalora, 2021). Some models are limited to examining only the content and method of delivery of the threat, for example when anonymously authored.

Risk assessment instruments used: these could be traditional violence risk assessment instruments or threat assessment instruments, where the main difference is the latter's inclusion of target information (Meloy et al., 2013). Structured professional judgement (SPJ) tools are recognised as best practice in threat assessment (Meloy et al., 2021).

Remote vs. in person threat assessment: some threat assessment models interview the target, subject, and witnesses, including the including family, friends, healthcare workers, police, and educational or work colleagues (Borum et al., 1999; Meloy et al., 2021). Others only work with remote information due to accessibility, concern about escalating risk to the victim, or unreliability (Van der Meer & Liekhuis, 2013).

Threat assessment output: the output the team is designed to produce, which may include levels of risk or concern, written reports, and management plans. Levels of concern are more common than levels of risk in threat assessment due to incomplete information and dynamic situations (Meloy et al., 2012).

Interventions

Violence prevention requires both assessment and risk management informed by this assessment (Meloy et al., 2021). Interventions can be carried out by the threat assessor or otherwise, and can include monitoring and supervision, treatment, and victim safety planning (Kropp & Cook, 2021; Tobin & Palarea, 2021)

In-house interventions: interventions that the threat assessment team themselves have the capacity and authority to carry out.

Outsourced interventions: interventions outsourced, referred, or recommended to other services or back to the referring agency.

Case management structure

Case review and monitoring structure and frequency*:* the threat assessment team often review and reassess the case, either themselves or by creating a monitoring network around the subject. This ensures interventions are effective in preventing violence and reducing levels of risk or concern (O'Toole, 2021).

Quality/standards assurance

Performance and efficacy evaluations: nature and frequency of evaluations of implementation, efficacy, or validity of threat assessment instruments.

Data collection and record keeping practices: whether and how case information is recorded, including any formal policies. Documentation is often crucial to protect the confidentiality of the information generated in assessment (Mohandie & Hoffman, 2021).

Data sharing between agencies: details on the problems of and solutions to data sharing between agencies where relevant, and how this is restricted by policies or legislation, including any exceptions to confidentiality (Mohandie & Hoffman, 2021).

Methodology

Inclusion criteria

This study reviewed case study literature that describes the structure and operations of threat assessment teams or models that have been implemented in practice. Therefore, inclusion criteria were:

1. Study concerns threat assessment: As opposed to (violence) risk assessment or risk and protective factors.
2. Study concerns an existing application of a threat assessment model or team: Included studies focus on the operations of a specific and existing threat assessment team. Excluded studies only described threat assessment instruments, or teams that should be used. Examples of the latter category are threat assessment 'principles', best practice guidelines from researchers or official bodies, or suggested models that are not at the time implemented, or were only pilot tested for research.
    a. Study describes a single framework: Reviewing the operations of one particular existing threat assessment model that the reviewer had experience with, rather than a descriptive summary of multiple existing frameworks or what tends to happen in a certain region, for example.
3. Study is in case study format: The primary purpose (within reason) must be describing the structure, operations, and development of the threat assessment team. Studies were excluded if this was given merely in a description introducing a paper that was mostly an efficacy or experimental evaluation, particular case example, or hypothetical application.
4. Study meets authorship criteria: Studies were written by someone working on the team or an embedded researcher within it. For example, excluded studies included reviews of open sources or practitioner surveys.
5. Study meets criteria for publication type. Examples of excluded studies were books, handbooks, webpages, conference proceedings, policy directives, and pieces of legislation. Handbooks and books were later reviewed for inclusion of individual chapters where possible.

Search strategy

Several strategies were used to find relevant literature. First, a literature search was carried out, identifying 7256 studies[1]. Five researchers excluded any studies that did not concern relevant problem behaviours or risk and threat assessment, leaving 3010 studies. One researcher then screened the title and abstract of the remaining studies according to the above inclusion criteria. This left 125 studies for full text screening, of which 25 studies were selected for inclusion.

[1] We conducted a keyword search of titles and abstracts in PsycNet and the National Criminal Justice Reference Service for papers published from database inception until 11th November 2021, restricted by English language. Key words searched for issues related to problems of interest (insider*" OR "violen*" OR "terroris*" OR "radicali*" OR "crim*" OR "recidiv*" OR "offen*" OR "extremis*" OR "aggressi*" OR "threat*" OR "arrest*" OR "reoffen*" OR "re-offen*" OR "assault" OR "femicide" OR "counterproductive workplace behav*" OR "stalk*" OR "sex*" OR "homicide*" OR "killing*" OR "attack*" OR "murder*" OR "harass*" OR "shoot*" OR "fixat*"), threat/risk assessment (("risk assess*" OR "threat assess*" OR "risk manag*" OR "threat manag*" OR "case manag*" OR "lethality assess*" OR "danger assess*" OR "assess* risk" OR "assessment of risk" OR "manag* risk" OR "management of risk" OR "risk instrument*" OR "risk classif*" OR "risk predict*" OR "actuarial" OR "structured professional judgement" OR "SPJ"), and evaluations ("evaluat*" OR "effect*" OR "outcome*" OR "program*").

Second, this was supplemented by a sift of chapters in both editions of the International Handbook of Threat Assessment (Meloy & Hoffman., 2013; Meloy & Hoffman., 2021) and other handbooks identified in the literature search. This yielded a further 14 studies. Thirdly, a Google Scholar search of keywords and phrases[2] was used to update the full search to March 2024, which resulted in the inclusion of a further 5 studies.

Finally, to ensure all ground was covered, and due to previous threat assessment systematic reviews obtaining more literature from reference lists than initial searches (Mitchell & Palk, 2016), all potentially included studies were subjected to a backward and forward citation search using Google Scholar, Semantic Scholar, and Research Gate (updated to March 2024). This was an iterative process, repeated until no further studies were included, and also involved exclusion of some previously included best practice studies that it was decided did not meet inclusion criteria 2. This resulted in an additional 19 studies.

In total, 47 studies fulfilled all criteria so were included in this review: 12 from the initial literature search, 11 from handbooks, 5 from a Google Scholar supplementary search, and 19 from citation searches. One extra report evaluating the UK Channel programme (Gill & Marchment, 2020) was selected for inclusion.

Included studies

The 48 included studies described 27 existing threat assessment models. These are categorised below, according to the primary setting in which they were originally designed to operate.

[2] Key words for Google Scholar search related to threat assessment ("threat assessment"), case study literature ("case study" OR "structure" OR "model" OR "framework" OR "operations"), and key settings ("violence" OR "schools" OR "workplace" OR "terrorism" OR "stalking" OR "fixated").

	USA		Europe		Australia
Schools	Comprehensive School Threat Assessment Guidelines	Cornell (2003) Cornell (2013) Cornell (2018) Cornell (2020a) Cornell (2020b) Cornell & Burnette (2021) Cornell & Heilbrun (2016) Cornell & Maeng (2017) Cornell & Warren (2024) Cornell & Williams (2011)	Networks Against School Shootings (Germany)	Fiedler et al. (2019) Leuschner et al. (2011) Leuschner et al. (2013)	
	Dallas Threat of Violence Risk Assessment	Ryan-Arredondo et al. (2001) Van Dyke et al. (2004) Van Dyke & Schroeder (2006)			
	Rappaport model	Rappaport et al. (2015)			
	Salem Keizer/Cascade model	Van Dreal & Okada (2021)			
Universities	Behavioral Intervention Team at Ozarks Technical Community College	Mrad et al. (2015)			
	Threat Assessment Team in a large Midwestern university	Scalora & Racionero (2021)			

Workplace violence	Coast Guard Investigative Service Threat Management Unit	Rutz (2021)				
	Employee Assistance Program	Holbrook et al. (2019)				
	Hughes Fullerton Critical Incident Team	Root & Ziska (1996)				
	Navy Criminal Investigative Service Threat Management Unit	Van Horn (2013)				
	Risk Assessment Team at Johns Hopkins University	Heitt & Tamburo (2005)				
	United States Postal Service Employee Assistance Program	Kurutz et al. (1996)				
Fixated threats/ protection of public officials	Los Angeles Police Department Threat Management Unit	Bixler et al. (2021) Dunn (2008) Dunn (2013)	Fixated Threat Assessment Centre (United Kingdom)	Barry-Walsh et al. (2020) James et al. (2013) MacKenzie & James (2011) Wilson et al. (2021)	Queensland Fixated Threat Assessment Centre and other Australian units	Pathé et al. (2018) Wilson et al. (2021)
	Mental Health Liaison Program consulting to the US Secret Service	Coggins & Pynchon (1998) Phillips (2008)				
	United States Capitol Police Threat Assessment Section	Scalora et al. (2008)				
Violent extremism	Community Connect	Ellis et al. (2022)	Channel programme and Vulnerability Assessment Framework (United Kingdom)	Gill & Marchment (2020)		

	FBI Behavioral Analysis Unit-1 Behavioral Threat Assessment Centre	Gibson (2023)	Dutch National Police investigative psychologists (Netherlands)	Bootsma & Harbers (2021)		
Mixed threat forms and problem behaviours (e.g. stalking, threats, general violence, targeted violence)	FBI Behavioral Analysis Unit model for analysing anonymous threatening communications	Simons & Tunkel (2013) Simons & Tunkel (2021)	Forensic Assessment and Case Management Unit within the Cantonal Threat Assessment and Management unit (Switzerland)	Guldimann et al. (2016)	Problem Behavior Program/Problem Behavior Clinic	MacKenzie & James (2011) McEwan & DarJee (2021) McEwan et al. (2013) Warren et al. (2005)
	San Diego Stalking Strike Force Stalking Case Assessment Team	Maxey (2002)				
	Willamette Valley Adult Threat Advisory Team	Van Dreal & Okada (2021)				

Threat assessment models

Schools

Comprehensive School Threat Assessment Guidelines

Summary
The Comprehensive School Threat Assessment Guidelines (CSTAG) model involves trained multidisciplinary teams preventing school violence by avoiding a profiling or zero tolerance approach and instead using threat assessment. Resources are reserved for the most serious threats, which are subject to in person interviews and potentially in-house interventions.

Threat assessment set up

Background and objectives
The CSTAG adopt a public health approach, where the focus is helping students to solve problems and conflicts that precede threatening or problematic behaviour, even if this behaviour would not have developed into an attack (Cornell, 2020b). Given the dynamic and situational nature of youth violence, the framework is about imminent risk for a specific threat, with a focus on risk reduction and prevention rather than risk prediction and measurement (Cornell, 2013; Cornell & Williams, 2011). This approach was inspired by FBI and United States Secret Service findings that violent students often faced common social, familial, and psychological problems, and usually communicated their intentions before an attack, giving an opportunity for intervention (Cornell, 2020a). The Virginia Youth Violence Project was formed to collaborate with school divisions to develop guidelines and field test these in Virginia schools (Cornell, 2003), leading to the CSTAG. The CSTAG approach responds to various issues unique to a school setting: the low base rate of violence but high level of everyday aggression; accounting for developmental factors in youth; and students being very receptive to instruction (Cornell & Burnette, 2021). Most importantly, threat assessment cannot focus on exclusion or legal action as schools have a duty to educate students (Cornell, 2020b). Zero tolerance policies are ineffective and implemented with racial bias (Cornell & Warren, 2024). So, the CSTAG is not a punitive zero tolerance policy and tries to avoid suspension (Cornell, 2013; Cornell, 2020a; Cornell & Warren, 2024). The main objective is to be flexible in treating all cases but resolving non-serious threats quickly, to focus resources on serious cases (Cornell & Burnette, 2021; Cornell & Heilbrun, 2016; Cornell & Warren, 2024).

Threat
School violence, inclusive of school shootings.

Basic information
- Country: United States
- Setting: School
- Date of formation: The Virginia Student Threat Assessment Guidelines were developed in 2001, published in 2006, and then updated and renamed as the CSTAG in a new manual in 2018 to show their broader potential for application. Threat assessment (though not necessarily using the VSTAG) was mandated in Virginia in K-

12 schools in 2013, and within 2 years all K-12 schools had threat assessment teams (Cornell & Maeng, 2017).
- Remit: Individual schools. This was preferred to teams with district-level remits, as it allows faster responses, better knowledge of the school and its students, more accessible reporting procedures, reduced conflict between schools and districts, and easier capacity for monitoring (Cornell, 2003; Cornell, 2018; Cornell & Burnette, 2021).
- Team location: Individual schools, to enhance familiarity with students and prompt responses (Cornell & Warren, 2024)

Team details

Specialist vs. multidisciplinary

Multidisciplinary: the core team and intervention possibilities combine several disciplines, partly driven by the fact that a law enforcement only approach risks criminalising student behaviour (Cornell, 2020a).

Team structure

The flexibility of the model dictates that the whole team is not necessarily involved in every case; non-serious cases are resolved quickly, to reserve full team resources for complex and serious cases (Cornell, 2020b; Cornell & Warren, 2024). The team is led by the school administrator with responsibility for student discipline (Cornell & Warren, 2024).

Core team

Disciplines in the core team (Cornell, 2020b; Cornell & Warren, 2024):
- School administration
- One or more mental health representatives such as a counsellor, school psychologist, or social worker. They are involved throughout the process from initial interview to evaluation for mental health services, and can provide counselling or conflict resolution in-house.
- Law enforcement representative: usually the school resource officer (SRO) or other police officer assigned to the school. SROs can respond to emergencies, investigate weapon possession, advise on gang activity or security measures, reassure the school community, and consult on law enforcement aspects such as security, criminal acts, and prevention-oriented policing (Cornell, 2003; Cornell & Warren, 2024).

Additional part time or consulted disciplines

Other potential team members can include (Cornell & Burnette, 2021; Cornell & Warren, 2024):
- Teachers: teachers are usually not in the team to protect their teaching responsibilities, but can provide information and are crucial sources of reported threats (Cornell, 2003).
- Nurses
- Other school staff
- Consultation with district level administrators or external resources if necessary

Training

Standardised interactive workshop training supplements a detailed manual including decision trees and mental health assessments (Cornell, 2020a; Cornell & Warren, 2024). Training focuses on the basics of school violence, rationale for avoiding zero tolerance policies, threat assessment procedures, relevant psychological factors, legal and ethical issues, and case exercises (Cornell, 2013). The Virginia Center for School and Campus Safety provides free regional workshops and ongoing training, and the University of Virginia research group created two educational programs (Cornell & Maeng, 2017).

Surveys and pre-post test studies in large samples found this training leads to better understanding of threat assessment principles, reliability in classifying cases, and lower support for zero tolerance exclusionary discipline policies (Cornell, 2020a;2020b; Cornell & Maeng, 2017; Cornell & Williams, 2011). This is true across all team disciplines (Cornell, 2020a).

Referrals structure

Case generation

Reported threats take many forms: direct or indirect from a third party; involving specific or diffuse targets; digital or written; and verbal or expressed through behaviour (Cornell, 2013; Cornell, 2020b).

Contact with referring bodies

According to the 2013 State of Virginia mandate, threat assessment teams must give guidance to staff and students on recognising and reporting threats (Cornell & Maeng, 2017). The University of Virginia research group also created an online education program to educate school communities on the process.

Threat assessment operations

Threat assessment process

The CSTAG threat assessment process is as follows (Cornell, 2020a; Cornell & Warren, 2024):

1. Interview: interviews by the principal or other team leader, of witnesses and the student making the threat to learn its exact content and context. If the communication or behaviour implies intention to harm, the case proceeds to step 2. If not, the case is closed but there may be interventions to address anger.
2. Decision of transient vs. Substantive: review of all information to determine whether the threat is transient (a reflection of humour, anger, or frustration, or with a retraction/apology) or substantive, meaning there is a threat to hit, fight, or beat someone up. If substantive, the case moves to step 4.
3. Resolving transient threats: if transient, the threat can be resolved with an apology, explanation, parent notification, or resolution of conflict, potentially with the use of counselling or disciplinary measures (Cornell, 2013). There is no comprehensive threat assessment (Cornell & Williams).
    a. Steps 1-3 are triage, where the team leader determines whether the threat can be resolved through limited action or requires all team members for full assessment. This can be completed in under an hour (Cornell & Williams, 2011).

4. Protect victim: for substantive threats, the first step is protecting the victim (with monitoring/supervision) and notifying the victim and both sets of parents or guardians.
5. Decision on level of seriousness of substantive threat: serious threats involve fights and assaults, while very serious threats involve threats to kill, inflict severe injury, rape, or use lethal weapons.
6. Respond to serious threat: this involves protective action including victim precautions and warnings, conflict resolution, student discipline, supervision, and parent notification for supervision outside of school (Cornell & Williams, 2011).
7. Respond to very serious threat: in addition to step 6, immediate protective action and safety evaluation. The student is suspended, kept in the principal's office, or placed elsewhere pending:
    a. Threat assessment team informing the target and the student's parents (Cornell, 2013; Cornell & Williams, 2011).
    b. Mental health evaluation for suitability for services or counselling.
    c. Law enforcement investigation (usually by the SRO) to determine if there is planning or preparation of a criminal act. They may advise on legal actions or protective security (Cornell, 2020).
    d. Creation of a safety plan to mitigate risk, using findings from the mental health and law enforcement investigations. This can include an individual education plan or assessment of disability.
8. Report: law enforcement and mental health evaluations culminate in a report detailing motivations, risk factors, and strategies to mitigate risk.
9. Implementation of safety plan and monitoring: safety plan is implemented and documented. The team maintain contact with the student and monitor them to determine if the intervention is working or needs revision.

Resources used in threat assessment

Throughout, the team considers all contextual information including age, capabilities, mental health status, and previous history of violence. The law enforcement investigation might look for weapon possession and evidence of planning or preparation (Cornell & Heilbrun, 2016). In 2008, legislation was modified meaning threat assessment teams have access to restricted information for serious threats, for threat assessment purposes only; this includes criminal history and health records (Cornell & Maeng, 2017).

Remote vs. in person threat assessment

The leader immediately conducts in person interviews with the student and any witnesses to further understand the threat and its context (Cornell, 2020a). These follow a standardised set of questions to consider the meaning and context of the threat beyond its literal content, and may be joined by mental health representatives (Cornell & Williams, 2011). There should also be interviews with the target to understand their perspective. If the threat is substantive, targets must be notified and there are clear guidelines on breaking confidentiality in this way (Cornell & Williams, 2011). If a threat is 'very serious', there are further interviews by mental health professionals. These include screening for urgent issues including psychosis or suicidality, followed by an evaluation to establish motivations, any mental health or counselling needs, and recommendations (Cornell & Williams, 2011). There are also potential interviews with teachers, family, or others who know the student to identify motivations and risk factors (Cornell, 2020b).

Threat assessment output

The main output is the safety plan, using recommendations combining findings from the law enforcement and mental health evaluations. Outputs within this are decisions on whether the threat is transient or substantive, and, if substantive, serious or very serious (Cornell, 2020a).

Interventions

In-house interventions

Mental health professionals can provide in-house counselling and conflict resolution (Cornell, 2020b). The SRO can advise on legal aspects, conduct criminal investigations, and provide protective security. More broadly, the team can warn and protect the target, talk to the student to resolve the conflict, issue disciplinary consequences, supervise, and suspend the student (Cornell, 2020a).

Outsourced interventions

Mental health team members can conduct mental health evaluations of suitability for services (Cornell, 2020b). The student might be referred for a special education evaluation or to external mental health services.

Case management structure

Safety plans include monitoring the student for a certain period, through contact with a team member to keep track of attendance and progress with mental health services, and reviewing or revising safety plans when necessary (Cornell, 2013; Cornell & Heilbrun, 2016; Cornell & Warren, 2024).

Quality/standards assurance

Performance and efficacy evaluations

The CSTAG have been subject to many empirical evaluations (Cornell & Warren, 2024). Initially, there were field test studies in Virginia schools of VSTAG training that determined they were practicable and efficient without leading to violent outcomes (Cornell, 2020a). There have also been controlled studies, finding that use of the CSTAG results in fewer long-term suspensions, less bullying, more students receiving counselling, and more parent conferences (Cornell, 2020b). In 2013 the VSTAG was recognised as the first evidence-based form of threat assessment by the National Registry of Evidence-based Programs and Practices (Cornell & Maeng, 2017).

Data collection and record keeping practices

The safety plan is fully documented (Cornell & Warren, 2024).

Dallas Threat of Violence Risk Assessment

Summary
The Dallas Threat of Violence Risk Assessment (DTVRA) is both a situational professional judgement tool and a school violence threat assessment process. This tool's inputs involve trained multidisciplinary teams conducting interviews. Intervention plans depend on risk level and focus on combining disciplinary consequences and support services for the student, along with avoiding harm to the student's future prospects.

Threat assessment set up

Background and objectives
The DTVRA model was developed based on United States Secret Service and FBI recommendations that schools should use multidisciplinary threat assessment (Van Dyke & Schroeder, 2006). The Dallas Independent Schools District (DISD) formed a committee to establish a districtwide threat assessment strategy, consulting with experts in psychology, school discipline, juvenile justice, and crisis management. The resulting policy moved away from profiling students to evaluating the level of risk of potential violence (Ryan-Arredondo et al., 2001). This policy involves a procedure for systematic assessment, direct intervention, and balance between using discipline and support services, where the actual DTVRA assessment tool is a minor part (Van Dyke & Schroeder, 2006).

Threat
Targeted violence in schools.

Basic information
- Country: United States
- Setting: School
- Date of formation: The committee developing the strategy was formed in 1997-8, and the DTVRA was first used in the 1998-9 school year (Van Dyke & Schroeder, 2006).
- Remit: Districtwide, implemented individually in each school.

Team details

Specialist vs. multidisciplinary
Multidisciplinary: the DTVRA is administered only by mental health and psychological professionals, but other disciplines are present in the team.

Team structure
The principal receives and triages the reported threat and may then refer the student to the counsellor or other mental health professional for DTVRA risk assessment (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006).

Core team
The core disciplines involved in the DTVRA process are:
- School principal
- School counsellor
- Psychological services

- Other psychological professionals including social workers, counsellors, nurses, or specialists

Additional part time or consulted disciplines
Teachers are interviewed and parents are encouraged to be involved throughout assessment and intervention (Ryan-Arredondo et al., 2001).

Training
Principals and counsellors are trained by the districtwide DISD Psychological Services Department and Office of Student Discipline (Van Dyke & Schroeder, 2006). The same information is given to both, but tailored to their different individual responsibilities, hence focusing on policies and codes of conduct for principals, and DTVRA use for counsellors. Principals are trained again each year, and counsellors already trained in the DTVRA receive refresher training from the psychological services professional assigned to their school.

Referrals structure

Case generation
After students make a verbal or non-verbal threat, this is passed on to the principal (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006).

Contact with referring bodies
Principals are responsible for training school staff and students on the policy. Psychological services supplement this with training on breaking the code of silence to encourage student reports (Van Dyke & Schroeder, 2006).

Threat assessment operations

Threat assessment process
The DTVRA wider process involves (Van Dyke & Schroeder, 2006):

1. Report: report of a threat is passed to the school principal.
2. Triage: the principal decides whether the threat is terroristic (involving imminent serious bodily harm, direct verbal threats, and capacity to carry these out). If so, they call police who determine arrests or charges under Texas Penal Code definitions (Ryan-Arredondo et al., 2001). The DTVRA still must be completed before the student leaves campus (Van Dyke et al., 2004). If the threat is less serious, the school maintains control and the principal refers the student for risk assessment. Either way, the principal informs the student's parents (Van Dyke et al., 2004).
3. Risk assessment using DTVRA, including interview: usually done by the counsellor or psychological services. This produces a judgement of low, medium, or high risk.
4. Intervention plan: developed with staff and parents, dependent on DTVRA risk level (Ryan-Arredondo et al., 2001):
    a. Low risk: interventions include parent conference, counselling, and follow-up by Student Support Teams.
    b. Medium risk: this could result in behavioural management plans, violence prevention programs, counselling, removal to on or off campus Alternative Education Programs, or referral to Youth and Family Centers for psychiatric, medial, or therapy treatment.

c. High or terroristic risk: psychological services complete a further assessment.

Resources used in threat assessment
When completing the DTVRA, counsellors have access to interviews and school academic and disciplinary records (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006).

Risk assessment instruments used
The DTVRA is a risk assessment instrument designed to be completed with readily available information to reach judgements quickly on violence risk and interventions plans. There are 19 risk factors including attack planning, previous behaviour, exposure to violence, support systems, and emotional instability (Van Dyke & Schroeder, 2006). Counsellors use information from interviews and records to rate the student low, medium, or high on each risk factor. These are tallied up and weighted towards more seriously presenting risk factors, or towards high risk in attack-related risk factors. When the DTVRA was designed, there was no previous DISD data collection for empirically validated risk factors, so this was essentially a pilot to create data for further development of the tool (Ryan-Arredondo et al., 2001). It is based on the SPJ framework and incorporates developmental and dynamic factors (Van Dyke et al., 2004).

Remote vs. in person threat assessment
There are in person interviews with the student, parents, and teachers, with standardised questions for each to target each risk factor of the DTVRA (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006). If low risk, the parent interview may be over the phone.

Threat assessment output
DTVRA output is a risk level (low, medium, or high) and associated intervention plan.

Interventions

The intensity of interventions is designed to meet the presenting level of risk, and work to combine disciplinary measures (which are usually necessary as the student has violated the Code of Conduct) and support services (Van Dyke et al., 2004).

In-house interventions
In-house interventions can be disciplinary measures (apology or expulsion), parent conference, or counselling by the school counsellor or psychological services provider (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006).

Outsourced interventions
Students can be referred to the Dallas County Juvenile Justice Alternative Education Program, campus-based Student Support Teams, youth and family centres, emergency psychiatric care or hospitalisation (Van Dyke et al., 2004; Van Dyke & Schroeder, 2006).

Case management structure

All students get follow-up case management from a campus-based Student Support Team, led by a counsellor (Ryan-Arredondo et al., 2001).

Quality/standards assurance

Performance and efficacy evaluations

Before this framework was developed, there was no empirically validated information on risk factors, due to a lack of database on student violence in the Dallas Independent Schools District (DISD) and the low base rate of youth violence (Ryan-Arredondo et al., 2001). The risk factors, aggregation procedures, and weighting in the DTVRA are arbitrary and not empirically validated, so more data is needed (Van Dyke & Schroeder, 2006). For evaluation, DISD Psychological Services keeps track of the submitted DTVRAs and Report Forms (Ryan-Arredondo et al., 2001) and there have been user surveys to evaluate efficient implementation of the DTVRA (Van Dyke et al., 2004).

Data collection and record keeping practices

The Threat of Violence Report Form completed by staff (previously named Behavior Report Form) summarises the threat, demographic information, precipitating factors, the target, DTVRA risk level, confirmation of parent notification, and action plan for support and discipline (Van Dyke et al., 2004). Copies of this and the completed DTVRA are placed in the counsellor file and student discipline file, with originals sent to the DISD psychological services. These are not kept in the student's cumulative folder, to prevent harming them in future schools or employers.

Rappaport school violence prevention model

Summary

The Rappaport model centres around the role of mental health clinicians to assess threats and build rapport, for a cohesive dynamic and to mobilise resources that are agreed upon for both the student's wellbeing and school safety.

Threat assessment set up

Background and objectives

Rappaport's model of school violence prevention stems from the consensus that zero tolerance approaches undermine cohesion, are ineffective in failing to distinguish between real and trivial threats, and lead to racial disparities in outcomes (Rappaport et al., 2015). It was inspired by the findings and recommendations of the Safe Schools Initiative that threat assessment should include an analytical approach and clinical formulation. The aim is to mobilise resources, create a cohesive school climate between staff, parents, and students, and to understand the student and/or family's subjective experience. Therefore, there is a key role for trained mental health assessors. By 2015, over 140 safety assessments following this model had been implemented.

Threat

School violence.

Basic information:

- Country: United States
- Setting: School
- Remit: School

Team details

Specialist vs. multidisciplinary

Multidisciplinary.

Team structure

The main role in this model is of clinicians, who share decision-making responsibility with school staff, assess threats with clinical formulations and recommendations, and mediate between family, students, and staff to diffuse tension. They balance and realign the potentially differing goals of support for the student and school safety.

Core team

The core team involves:

- School administrator
- School resource officer
- Clinician/consultant: school psychologist/guidance counsellor/clinical social worker

Training:

Clinicians must be knowledgeable on Safe School Initiative protocols, and familiar with school and external resources.

Referrals structure

Case generation
Cases are referred to the team following indirect threats, direct threats, or assault without weapons. This behaviour can encompass swearing at teachers, property destruction, fighting, assaulting staff, inappropriate sexual behaviour, or online threats.

Threat assessment operations

Threat assessment process
1. Referral: a threat is referred to the clinician.
2. Triage: if there is imminent risk of harm, they immediately refer to the police. If there is no imminent risk but a high level threat needing thorough evaluation, they refer to the multidisciplinary team for psychiatric safety assessment.
3. Assessment: by the team to understand context of the behaviour and decide whether the student can return to school. Clinician suggests intervention recommendations.
    a. The first step in this assessment is always student safety and considering immediacy of harm potential.
    b. The clinician builds a therapeutic alliance to understand motivation and context, through considering the incident, current mental state, involvement with bullying or drug/alcohol use, psychosocial stressors, domestic violence exposure, and other contexts.
    c. The assessment is objective, but also subjective through understanding the student and family's perspective.
4. Formulation report: alongside meeting with the school, family, and/or student to discuss recommendations, treatment, and educational planning.

Resources used in threat assessment:
Assessment includes review of school records (incident report, academic transcripts, individualised education program, psychological testing), and discussion with school personnel or other mental health practitioners.

Remote vs. in person threat assessment
There are interviews with staff, the student, mental health practitioners, and parents/guardians to understand all perspectives. Interviews with students centre around building rapport, explaining limits of confidentiality, assessing context and safety. For family and school staff, they centre on gauging receptiveness for certain interventions or resources.

Threat assessment output:
The output is the written consultation consisting of a formulation report, alongside a meeting with relevant people to discuss recommendations and treatment.

Interventions

Outsourced interventions
The clinician is familiar with external resources and able to put the student in touch with these. Recommendations may include mental health treatment, home-based services, behavioural analysis, academic accommodations, medication, or alternative education programs.

Quality/standards assurance

Performance and efficacy evaluations
Initial findings of evaluative studies show that parents and students initially perceive the school as overreacting or being aligned against them, but the safety assessment process facilitated by the clinician corrects this dynamic.

Data sharing between agencies: details on the
Confidentiality limits are explained in interviews. The written formulation is for the school, meaning information shared by family to clinicians is not confidential.

Salem-Keizer/Cascade model

Summary

The Cascade model of school violence prevention involves an on-site level 1 multidisciplinary team that can escalate cases to a community-based and multi-agency level 2 team for advice. The level 2 team provides assessment and consultation on potential agency interventions.

Threat assessment set up

Background and objectives

The Cascade model was led by Salem-Keizer public schools and designed through research, practitioner recommendations, and committees of experts in education, mental health, law enforcement, and juvenile justice (Van Dreal & Okada, 2021). It is a multidisciplinary and multi-agency collaboration avoiding profiling and focussing on relieving the circumstances (both situational factors and risk factors) that worsen the risk of future violence. The model focusses on assessment, prevention, supervision, and intervention through access to community resources. There are two tiers: a level 1 school-based team, and then escalation to a level 2 community team.

Threat

Direct threats, indirect threats, potential for aggression and dangerous activities, behaviours, or communications. The model does not apply to suicide, sexual misconduct, or fire setting unless there is an accompanying act of extreme aggression, as there are alternative school protocols for these.

Basic information

- Country: United States
- Setting: School
- Date of formation: The Mid-Valley Student Threat Assessment Team was formed in 1999, launched in 2000, and has since been named the Salem-Keizer or Cascade model due to implementation in other jurisdictions.
- Remit: Threats made by students.
- Team location: Level 1 is school site-based, but level 2 is community-based.

Team details

Specialist vs. multidisciplinary

Multidisciplinary and multi-agency: both level 1 and particularly level 2 teams are multidisciplinary consultative and collaborative groups to assess solutions, supervise, and prevent violence. This does create some issues regarding lack of resources in certain agencies, differing philosophies, lack of data sharing or confidentiality policies, and funding limits, but each agency is committed to supporting the team's efforts.

Team structure

The level 1 team is based at the school. There is a core team, and potential additional personnel brought in dependent on the threat. The level 1 team are case managers, with authority and responsibility for final decisions. Students may be referred to the community-based level 2 Student Threat Assessment Team (STAT). This team cannot mandate

interventions or override any agency's policies, and are more consultative in helping to review cases, recommend interventions, and advise on follow-up. Within the STAT, there is an investigative team that carries out assessment. The STAT meets weekly for assessment and review of cases.

Core team

The level 1 school-based team comprises the following:

- Administrator
- School counsellor or mental health professional, other teachers or support staff, or consulted local mental health agencies
- School resource officer or other law enforcement representative

The wider level 2 STAT comprise the following agencies:

- K-12 school district personnel
- Law enforcement
- Public mental health services
- District attorney's office
- Victim advocacy services
- Juvenile justice
- State youth authority

Within this, the level 2 community investigative team comprises representatives from:

- Education, the team leader: a school psychologist or education specialist. Education leads the implementation and response due to the importance of the student's school connection even if the assessment started in another area, such as law enforcement. As the team leader, they coordinate the process and materials, and present to the STAT.
- Public mental health services: these do not carry out clinical evaluations or treatments, and are instead consultative. They assess threats from clinical perspectives, translate psychiatric terminology and diagnoses, and provide knowledge of community mental health evaluation and intervention options.
- Law enforcement: they take an active role in providing knowledge on specialised assessment, targeted violence risk factors, intervention possibilities, criminal behaviour expertise and attack related behaviours. They go beyond gathering information to compiling it for the team and applying their expertise.

Additional part time or consulted disciplines

In the level 1 site-based team there may be others who know the student, including teachers and coaches, campus security, parents, or other staff.

The level 2 broader team can also include other youth agencies for consultation, including child welfare services or other case managers. The investigative team brings in additional team roles as necessary.

Training

The level 1 team must be trained on level 1 process and assessment procedures, using training available online. The level 2 STAT should all be highly trained in investigative assistance, assessment, consultation, and resource provision. Further, the level 2 investigative team should each be trained well in applying their respective discipline to threat

assessment, including psychoeducational assessment, behavioural assessment, multidisciplinary collaboration, and crisis intervention.

Referrals structure

Case generation
A threat may be direct, veiled, indirect, or an act of aggression. There is a centralised reporting structure for the level 1 school-based team.

Contact with referring bodies
Referral guidelines provide a threshold for reports, and details of what threat assessment can and cannot offer, clarifying that it is not prediction nor a checklist.

Threat assessment operations

Threat assessment process

1. Referral: threatening situation identified by the level 1 team.
2. Initial response: the level 1 team may initiate a protective response if there is imminent danger. They may ask law enforcement to initiate a criminal investigation, or decide to carry out level 1 threat assessment.
3. Level 1 threat assessment:
    a. Student and staff safety precautions: including potentially detaining students and restricting access to belongings. If any imminent danger posed, they call law enforcement and follow school district procedures.
    b. Team assessment scheduled: with student interview completed before the meeting. The student should not attend the meeting. Staff familiar with the student either attend or are given a questionnaire.
    c. Notification of parents: and potentially inviting parents to the team meeting if constructive, otherwise they must be interviewed in person.
    d. Assessment: following set protocol which involves intervention strategies and assessment questions exploring context, situational factors, information from interviews, and collateral information. The aim is to determine the risk, urgency, and severity of potential injury using information on the target, planning, and capabilities.
    e. Precautions: potentially notifying and protecting the target, supervising the student, calling law enforcement, initiating protective security, and contacting the level 2 team for consultation or further assessment.
    f. Parent notification: of concerns, the safety plan, and referrals to any agencies.
    g. Evaluation of further options for supervision: unique to each case, based on situational factors, and on principals of fairness.
    h. Decision about proceeding to level 2, following published criteria: criteria include dangerous weapons, team inability to answer certain protocol questions, safety concerns about severity of injury, evidence of planning, or exhausted school resources.
4. Level 2/STAT assessment if necessary
    a. Triage criteria for which cases to take on: including level of aggression, communications, plans, target specificity, and availability of weapons.
    b. Information-gathering: lead looks at records, situational information, level 1 information, and interviews.

c. Assessment: level 2 investigative team assesses at school site using level 1 protocol but in more depth. They collect information, meet the level 1 team, and help with management plans.
d. Report to STAT: lead coordinates information and presents back to STAT at scheduled weekly meetings.
e. STAT meeting: review with larger team where case manager presents updates, investigative team present their assessment results, and there is further assessment or consultation. Level 1 team can attend in person or via phone.

Resources used in threat assessment
Law enforcement in level 2 can look at criminal records and police contacts, and use search and seizure, arrest, protective action, interviews, phone, or social media data.

Risk assessment instruments used
Mental health professionals in level 2 investigative team often uses empirical assessment protocols.

Remote vs. in person threat assessment
The level 1 team administrator or SRO interviews the student and witnesses before the level 1 meeting, and potentially their teachers and staff, following set questions and questionnaires. In level 2, if a mental health evaluation is needed, the mental health professional interviews the student, their family, and staff to find mental health conditions, motivations, and intervention needs.

Threat assessment output
Outputs are safety plans from both teams.

Interventions

In-house interventions
The level 1 team are the case managers with authority over interventions. They can detain the student and restrict access to belongings.

Outsourced interventions
The level 1 team can refer to law enforcement, school district administrators, community services, and level 2 if necessary. The level 2 team is consultative so does not focus on providing treatment. The mental health professional can conduct mental health evaluations, and then refer to other options in school or out of school.

Case management structure

In the level 1 system there is ongoing monitoring to determine any changes in risk factors or level of concern following interventions. The STAT level 2 weekly meetings are used to review new, current, and old cases for follow-up, and will provide further consultation if situations change.

Quality/standards assurance

Performance and efficacy evaluations

The University of Oregon Institute on Violence and Destructive Behaviour produced a study of perceptions of users of the Cascade model, where almost all administrators and counsellors claimed it identified potentially dangerous students well and was beneficial for school safety.

Data collection and record keeping practices

In levels 1 and 2, everyone involved in supervision and intervention keeps copies of recommendations to refer to, and communications with partners are documented. Official threat assessment information is kept in a confidential envelope in the student's file, with a second copy in another location (often the security office or district administration office).

Data sharing between agencies

Data sharing is a source of problems in a multi-agency collaboration. For example, if there is a criminal investigation, only information that does not compromise the investigation and is necessary for threat assessment and safety planning is given to the team.

Networks Against School Shootings

Summary
The Networks Against School Shootings (NETWASS) model was borne out of the Berlin Leaking Project. It focuses on using leakage and warning behaviours as points of intervention and support for students who are either in individual crisis or on a critical development path towards violence. It uses a triage system, which involves interdisciplinary teams that consult with community agencies, and forms a professional network of agencies to coordinate interventions.

Threat assessment set up

Background and objectives
NETWASS is a school violence prevention program initiated by leakage, threats, and concerning behaviours (Fiedler et al., 2019; Leuschner et al., 2013). The model combines threat assessment with crisis prevention, to emphasise supporting students in crisis alongside violence prevention, where severe targeted violence is the end point of a development path of psychosocial, situational, and structural factors (Fiedler et al., 2019). Various factors unique to German schools and youth violence necessitate a tailored approach (Fiedler et al., 2019; Leuschner et al., 2013). In particular, the model does not directly copy the United States 'threat assessment' approach, to avoid stigmatising students as 'threats' and instead using language of crises and support. However, inspiration was taken from the Virginia model of the assessment process focusing on behaviour rather than risk profiles. The model is based on contemporary research regarding threat assessment, emergency response, and early intervention (Fiedler et al., 2019). Main aims are to enhance staff awareness of reporting leakage behaviours, increase confidence in handling these, and ultimately to intervene by responding to leakage as an indicator of violence (Leuschner et al., 2013).

Threat
School shootings and severe targeted violence (Fiedler et al., 2019).

Basic information
- Country: Germany
- Setting: School
- Date of formation: A university research team developed the program in 2009-2013 (Fiedler et al., 2019).
- Remit: Nationwide, implemented within each school (Fiedler et al., 2019).

Team details

Specialist vs. multidisciplinary
Interdisciplinary (Leuschner et al., 2011): the core team is limited and small, but external networks and consultation are encouraged, and multi-agency networks are formed for interventions. All perspectives are considered, and any decision is made by the whole team.

Team structure:
The Crisis Prevention Team (CPT) is led by the Crisis Prevention Appointee, who has responsibility for convening the team and initial information-gathering (Fiedler et al., 2019).

Core team

Disciplines in the CPT include (Fiedler et al., 2019; Leuschner et al., 2013):

- School principal
- Crisis Prevention Appointee: the principal or a delegated teacher or social worker, who has authority in case of disagreement. This individual should be accepted by the school community and the role should be taken on by more than one person to cover absences.
- Other staff with NETWASS training
- Potentially homeroom teachers, social workers, or other staff who know the student

Additional part time or consulted disciplines

NETWASS recommends that external disciplines (including law enforcement) are present in the CPT for consultation, but the time of their involvement is decided by the principal unless immediate police action is needed (Leuschner et al., 2013). NETWASS also involves creating a professional network in the community of collaborative partners, who can each be invited to join the CPT when required. These include:

- Law enforcement: however, there is resistance to including police in the CPT as in Germany they must immediately file a charge if a statutory offence is committed
- School psychologists: responsible for more than one school so may not have resources for all cases
- Youth welfare officers
- Mental health professionals

Training

All members are trained, and there have been evaluation studies analysing which training formats are most effective, and showing that training increases knowledge and skills (Fiedler et al., 2019).

Referrals structure

Case generation

The process is initiated by leakage behaviour, which can be threats (verbal, gestural, or violent incidents) or other behaviours (including preoccupation with weapons or past shootings, or a collection of risk factors). This separates NETWASS from the Virginia model that only responds to threats (Leuschner et al., 2011). The teacher or student that observes this warning behaviour reports to staff who, if they cannot explain the behaviour by the context, reports to the Prevention Appointee (Fiedler et al., 2019).

Contact with referring bodies

NETWASS centres on building trust between students and staff to break the code of silence and encourage reporting not just to prevent violence but get support for students in crisis (Leuschner et al., 2013). The CPT trains all staff for identifying and responding to students in crisis or exhibiting concerning behaviours (Fiedler et al., 2019).

Threat assessment operations

Threat assessment process

The NETWASS process includes (Fiedler et al., 2019; Leuschner et al., 2013):

1. Report: leak comes to the attention of staff.

2. Triage: staff forward to the Prevention Appointee if the threat or behaviour cannot be explained away by the situation or context, and there are references in the threat to a critical development towards violence. This ensures that cases where there is no real intention to harm are not passed on.
3. Prevention Appointee information-gathering: they condense information from multiple sources, evaluate, and offer recommendations. They decide if the threat can be explained by the situation, or more information is needed, and choose to call the CPT into action if there are indications the student is in crisis.
4. CPT assessment: the CPT first conducts a collaborative and evidence-based threat assessment based on the United States Secret Service recommended questions.
5. CPT evaluation: they make a judgement using risk factors to determine whether the student is in a psychosocial crisis or on a critical development path towards violence, and requires further action. They consider all available information including individual vulnerabilities, social strain factors, and protective factors.
6. Intervention: chosen based on the evaluation. Ideally the intervention resolves the situation, minimises risk factors, and maximises protective factors.
7. Case monitoring: one or more people monitor and report back to the CPT on progress and/or key events or changes in circumstances.

Resources used in threat assessment

In the Prevention Appointee's information-gathering, they examine reports, class register entries, and student files (Leuschner et al., 2013).

Risk assessment instruments used

CPT assessment is based on the United States Secret Service's 11 questions involving motive, communication, intentions, capacity, and hopelessness (Leuschner et al., 2013).

Remote vs. in person threat assessment

The Prevention Appointee should interview the reporting staff member and parents to establish cause for concern, family, schoolwork, social situation, and to correct any miscommunications (Fiedler et al., 2019; Leuschner et al., 2013).

Threat assessment output

Output is a final decision on the student being in an individual crisis or critical development towards violence, and an intervention or case management plan.

Interventions

In-house interventions

Potential in-house interventions include parent-teacher interviews (Leuschner et al., 2013). Rather than intervention, the main role for the school and CPT is to initiate support services and then monitor progress (Leuschner et al., 2011).

Outsourced interventions

The main source of intervention opportunities is the professional network of regional community agencies. The student can be referred for antibullying programmes, psychotherapist services, or police involvement (Leuschner et al., 2011; Leuschner et al., 2013).

Case management structure

At least one staff member is assigned to monitor the student's progress and report back to the CPT to see if intervention measures are effective (Leuschner et al., 2013). This should be someone who can contact the student and has a positive relationship with them, including homeroom teachers, social workers, or counsellors. Case management ends when it is decided that the student is no longer in critical development.

Quality/standards assurance

Performance and efficacy evaluations

A quasi-experimental evaluation study of 108 schools was the first large-scale evaluative study of threat assessment in Europe, and showed the NETWASS approach was feasible and effective (Fiedler et al., 2019). Those with NETWASS training had improved staff expertise, confidence in evaluating threats, identification of students in crisis, and ability to provide support. Training also increased general feelings of school safety and positive experiences with external services.

Data collection and record keeping practices

Internal reporting of leakage is made in writing, so that teachers give sufficiently serious answers and avoid hasty conclusions. This allows more information on critical development for the Prevention Appointee. The USSS threat assessment recommended questions are used to record answers and risk or protective factors. NETWASS handles data carefully to avoid stigmatising students and respect data protection regulations.

Universities and Higher Education

Behavioral Intervention Team at Ozarks Technical Community College

Summary

This Behavioral Intervention Team (BIT) model is a collaboration between a multidisciplinary team in a community college and the training clinic of a doctoral programme in clinical psychology, who provide consultation and assessment.

Threat assessment set up

Background and objectives

This mutually beneficial partnership provides a threat assessment service for a community college without a psychological or medical department, and experience for doctoral students (Mrad et al., 2015). Objectives are to prevent crises before they occur through outreach and education, a unified referral system, assessments, putting students in contact with accessible services, and monitoring for behaviour patterns.

Threat

Targeted violence.

Basic information

- Country: United States
- Setting: Higher education
- Date of formation: BIT formally started in 2010 following a year of development and training, and a contractual collaborative relationship was formed in 2011.

Team details

Specialist vs. multidisciplinary

Multidisciplinary: a collaboration between a multidisciplinary team in a university, and clinical psychologists. Within the BIT, team members have combined experience with disability support, rehabilitation, law enforcement, military, student conduct, and counselling.

Team structure

The BIT meets weekly for 2-3 hours to receive new incident reports, agree on action plans, and provide updates. Once a month, the forensic psychologist and one doctoral student from the partner clinic attends these meetings. They are also available for quick threat assessment and immediate response in high-risk situations, so there is capacity for daily collaboration and consultation.

Core team

The BIT community college team contains the following community college staff:

- Counselling: Director of counselling
- Academic and administration: Dean of students, assistant registrar, and full-time faculty member
- Assistant dean of disability support services
- Security: college director of safety and security

Additional part time or consulted disciplines
Beyond the BIT core team, they consult the clinical psychology doctoral programme. One forensic psychologist consults to the BIT and meets with the BIT at least once a month, along with doctoral students.

Training
All BIT members are masters or doctoral level professionals with experience in higher education student affairs and administration. Combined, the BIT have experience in disability support, rehabilitation, law enforcement, military, student conduct, and counselling.

Referrals structure

Case generation
Members of the college community (employees, visitors, and students) report using an online reporting system which is secure, easy to access, and potentially anonymous.

Contact with referring bodies
The BIT provides educational outreach, published guidelines, and regular professional development activities for the campus community to spread their objectives, so that everyone knows what, how, and why to report.

Case management structure

Weekly BIT meetings include progress updates on open cases.

Threat Assessment Team at a large Midwestern university

Summary

The Threat Assessment Team (TAT) is a multidisciplinary partnership between departments of a university, with a wider team who are consulted upon for complex cases.

Threat assessment set up

Background and objectives

The TAT was developed follow high profile campus shootings, during a widespread acknowledgment of the need to incorporate mental health agencies into threat assessment for education settings (Scalora & Racionero, 2021). For a successful TAT, technical knowledge of threat assessment is necessary but insufficient, as consultation skills and partnership experience are also required. The model was based on literature and consultation concerning university police cases of targeted violence and concerning behaviours. It is a flexible model, that considers behaviour rather than profiling.

Threat

Troubling behaviours towards campus stakeholders and the campus in general, that could cause harm, threats to life, or serious damage.

Basic information

- Country: United States
- Setting: Higher education

Team details

Specialist vs. multidisciplinary

Multidisciplinary: a core multidisciplinary team with additional consulted departments. Law enforcement leadership is crucial, but the TAT also must support community values and avoid being overly punitive. Threat assessment centres on de-escalating conflict and employing interventions that are fair and respectful. Therefore, psychological consultants are fully integrated members of the team.

Team structure

The core TAT of police personnel and psychological consultants work on all cases and consult with the wider team for more serious or complex cases.

Core team

The core TAT are those who have decision-making power in concerning situations, and their purpose is to facilitate communication and facilitate access to resources:

- Police: overseen by the Chief of University Police, who is the team leader.
- Psychological consultants: who meet stakeholders to develop team structure, provide team training, safeguard privacy and confidentiality, perform case consultation, develop risk judgements and management strategies, liaise with the mental health community to exchange information and access resources, and conduct program evaluations and research.

Additional part time or consulted disciplines

Additional disciplines can include the following, who assist when required:

- University administrators
- Faculty
- Legal counsel
- Human resources
- Student or judicial affairs
- Campus mental health services

Training

Psychological consultants must be trained in threat assessment, while police personnel must have experience in conducting investigations and sourcing background information. The psychological consultants also give training on risk factors, mental health issues and services, and management strategies, to the wider team and university police.

Quality/standards assurance

Performance and efficacy evaluations

This multidisciplinary model also draws on the research experience of psychological consultants, who conduct program evaluation research. They evaluate effectiveness of activities, outcomes of threat assessment and management, and underlying trends in threats, motivations, or risk factors. Lessons learned from such research include the importance of continuous training for collaboration due to high turnover, continuously educating stakeholders in reporting procedures, and ethical issues in the frequent indirect assessment of behaviour by mental health professionals.

Workplace violence

Coast Guard Investigative Service Threat Management Unit

Summary
The Coast Guard Investigative Service (CGIS) Threat Management Unit (TMU) is a behavioural analysis program aimed to facilitate intervening in concerning behaviour before violence occurs. The TMU is a specialised unit of agents who provide consultation on CGIS cases, involving triage and comprehensive threat assessment to deliver a set of recommendations.

Threat assessment set up

Background and objectives
The CGIS TMU was created in response to a CGIS workplace homicide in 2012 and was based on best practice from international experts and research (Rutz, 2021). As there was no one-size-fits-all approach, the TMU is a tailored model that focuses on flexibility, a clear timeline of input, investigation, and output, being people-focused, and having monitoring systems. The TMU has a dual role of being the subject matter experts on threat assessment and management, and internal consultants for any related cases in the CGIS.

Threat
Targeted violence, including workplace violence, stalking, sexual predation, ideological radicalisation, suicide, and intimate partner violence.

Basic information
- Country: United States
- Setting: Military
- Date of formation: CGIS created the TMU in 2013

Other involvements
The TMU also supports protective intelligence for CGIS officials and dignitaries, the CGIS insider threat program, and other CGIS investigations.

Team details

Specialist vs. multidisciplinary
Specialist: The TMU itself is a specialised team of military special agents, who can consult with clinical forensic psychologists. However, the management plans focus on interdepartmental collaboration. The TMU uses the military's many services by finding internal partnerships and gaining expertise and perspectives from various disciplines including human resources, Employee Assistance Program, Family Advocacy Programs, legal counsel, special agents, medical officers, chaplains, and security managers.

Team structure
The TMU team provide consultation to CGIS agents, legal offices, and others. The TMU assists in ensuring that all advice is considered and that implementation plans are easy to follow. Each case is assigned to a primary and secondary TMU special agent. The primary agent leads and manages communication, information-gathering, and identifying

investigative tools. Both review all information for threat assessment if relevant, sharing their observations and conclusions.

Core team
The core is a small, centralised, and specialised team of military special agents.

Additional part time or consulted disciplines
TMU can coordinate access to the CGIS clinical forensic psychologist to help with threat assessment and management.

Referrals structure

Case generation
Cases are referred to the TMU by the CGIS via phone, email, or a formal request on the CGIS case management system. Reported behaviours can include allegations of violence, threats, stalking, concerning communications, or unusual approaches to CGIS officials.

Contact with referring bodies
The TMU provides information and training to CGIS field offices and stakeholders on threat assessment and management, and how to respond to various situations including stalking, domestic violence, and suicide.

Threat assessment operations

Threat assessment process
1. Referral: CGIS receives a report and refers this to the TMU.
2. Screening: The TMU provides initial advice and looks for any concerning or warning behaviours. The case then goes to either consult & triage or comprehensive violence threat assessment.
3. Consult & triage: this can involve further information-gathering or meetings, and may result in a report. This is not threat assessment and does not produce a judgement on level of violence risk concern. Threat assessment may be recommended.
4. Comprehensive threat assessment: this is an indirect assessment using information leading up to this point. The assessment might change as more information is received and analysed. This culminates in a document with the judged level of concern for violence and a threat management plan, which aims to help the CGIS make protection or management decisions.
5. Report: report on either screening, triage, or threat assessment is passed back to the referrer, emphasising that this is a dynamic report. There is often a phone call or in person meeting to discuss findings and recommendations.

Remote vs. in person threat assessment
The TMU do not conduct interviews themselves but provide advice on core questions to consider in interviews by case agents, investigators, and commands. These focus on obtaining biological, psychological, and social information about the person of interest.

Threat assessment output
The output is a report given to the referrer, either from screening, triage, or comprehensive threat assessment. For the latter, this includes the level of concern and a management plan.

The primary special agent drafts a report, which is reviewed by the secondary agent and signed off by both.

Interventions

In-house interventions

As a consultation resource, TMU management plans comprise advice and recommendations only.

Outsourced interventions

The management plan focuses on integrating organisations to help the person of concern build a physical, social, and organisational environment of support systems. These offer intervention opportunities and early warning monitoring systems so are constantly evaluated. Recommendations and advice within this utilise the wider resources of the CGIS and can include military protection orders, Protective Security Detail, safety planning advice, check-ins, support for prosecutors, mental health evaluations, referrals to Family Advocate Program, medical evaluations, and removal of firearms.

Case management structure

A key finding from experts and research in building this model was the need for ongoing case management, so the threat management strategy is constantly evaluated for effectiveness and improvements. The TMU's multidisciplinary approach can establish networks and feedback loops around a subject for monitoring purposes, encouraging the use of medical and mental health services. There should be regular meetings to monitor behaviour and decide next steps, but these can be resisted when a case is old; the TMU can therefore conduct independent check-ins with local Crisis Intervention Team for updates.

Employee Assistance Program

Summary

Employee Assistance Program (EAP) professionals play an important role in workplace violence threat assessment through helping assess potential for violence and working with the employee and management to mitigate this potential.

Threat assessment set up

Background and objectives

The EAP has a wide-ranging role in enhancing employee wellbeing, mediation, and counselling (Holbrook et al., 2019). For organisations with an EAP, they are also crucial in workplace violence prevention and threat assessment teams.

Threat

Workplace violence.

Basic information:

- Country: United States
- Setting: Workplaces with EAP
- Remit: Employees

Other involvements

EAP professionals are also involved in critical incident response including debriefing and counselling. Beyond violence, they provide counselling, help to management with disciplinary issues, conflict resolution, and training, among other activities.

Team details

Specialist vs. multidisciplinary

Multidisciplinary: they operate within a multidisciplinary threat assessment team, where their role is counselling and providing mental health perspectives.

Team structure

When the EAP is contacted about a workplace threat, they take the lead in assessment and management.

Core team

Threat assessment teams with EAP representatives include at least:

- EAP professionals: clinical social workers, psychologists, psychiatrists, peer counsellors, or those with advanced degrees in behavioural health.
- Security personnel

Referrals structure

Case generation

Employees who have been threatened or witnessed threatening behaviour report to their manager, who refer to the EAP. EAP professionals can also refer workplace threats that emerge during standard counselling.

Threat assessment operations

Threat assessment process

1. Referral: employee refers to manager.
2. Escalation to EAP: management contacts EAP, where the first priority is immediate action to protect the target.
3. EAP recommendation: of multidisciplinary team assessment.
4. Team assessment.
5. Referral to services: EAP can refer to external services.
6. Further medical evaluation: if very serious, EAP can arrange for threat assessment by a forensic clinician. EAP may also consider another medical evaluation by a previous treatment provider or external specialist, e.g. for chemical dependence.
7. Case management.

Remote vs. in person threat assessment
EAP interviews the employee of concern.

Threat assessment output:
The main output is referral to services.

Interventions

In-house interventions
Some recommended services are in-house: EAP counselling of the subject or others affected, security precautions, and HR options (e.g. administrative leave and restricted access to site).

Outsourced interventions
Other recommended services are external, e.g. community anger management resources.

Case management structure

If treatment is needed, EAP case manages until all team and services members agree there is no threat of harm in the workplace.

Quality/standards assurance

Data sharing between agencies
EAP are bound by confidentiality generally, but there are releases of information signed that clearly state exceptions, including in workplace violence threat assessment cases where the EAP professional must report to the employer regarding the employee's safety to return to work.

Hughes Fullerton Critical Incident Team

Summary

The Hughes Fullerton Critical Incident Team (CIT) model was a workplace violence prevention program developed by a commercial organisation whilst it was downsizing its workforce. It involved cross-functional teams incorporating external mental health support in evaluations and counselling interventions.

Threat assessment set up

Background and objectives

Hughes Fullerton implemented several plans during a period of downsizing to mitigate its effects on psychological distress and violence (Root & Ziska, 1996). They created a People Team, which encompassed several sub-teams, including the CIT. The overarching philosophy was that workplace violence could be avoided if people were treated fairly, with respect and dignity. Other guiding objectives included ensuring support and understanding from executive leadership, a policy of zero tolerance towards violence, a cross-functional CIT, training managers and superiors in identifying violence potential, meeting regularly as a team, confidentiality, employing outside mental health professionals, and careful documentation.

Threat

Workplace violence during corporate downsizing, within a broader aim of preventing any kind of workplace trauma.

Basic information

- Country: United States
- Setting: Commercial organisation
- Date of formation: The People Team existed for 17 months between 1994 and 1995 during a period of downsizing at Hughes Fullerton, and the model was then extended to other Hughes sites.
- Remit: Employees at Hughes worksites.

Team details

Specialist vs. multidisciplinary

Cross-functional: the core team involved many departments and disciplines.

Team structure

A major principle was that the CIT should meet regularly, with each team member sharing their perspective on a given case.

Core team

The CIT comprised:

- Security
- Human resources
- Medical
- Employee Assistance Program

Additional part time or consulted disciplines

A major principle was that the CIT recognised the need for outside mental health professionals, including psychologists and psychiatrists, through the Employee Assistance Program (EAP).

Training

The CIT were given extensive training by EAP professionals and by the University of South Carolina Center for Crisis Management, sponsored by corporate human resources. Training focused on workplace violence, how to recognise it, and the function of the CIT. Training was ongoing due to high turnover in team membership.

Referrals structure

Case generation

Employees were told to report any threats to their supervisor, who then called the CIT on their, or another supervisor's, behalf.

Contact with referring bodies

A major objective of the CIT was to train managers and supervisors in identifying concerning behaviours. Training in workplace violence was given to supervisors, security, human resources, and department administrators. Hour long training was given to between 50-100 people over two weeks, by EAP professionals and endorsed by executive management. Training focused on risk factors and warning signs for potential violence, and company procedure for what to do when violence risk is identified. Shortly after this training was provided, reports increased, implying some level of success. With more time, the CIT would have trained more people that have contact with lots of employees, including secretaries and union representatives.

Threat assessment operations

Threat assessment process

1. Referral: CIT received a report of a threat from a supervisor.
2. Meeting: depending on the severity and urgency of the threat, the CIT usually met later that day and involved whoever was relevant including the reporting supervisor or manager.
3. Investigation: human resources, security team members, or both, investigated the threat. Subjects may be immediately excluded from the worksite, usually with pay.
4. Psychological evaluation: EAP would generally refer the subject for a psychological evaluation, where they were assessed by a psychologist experienced in workplace violence and psychological testing.
5. Meeting: after the mental health assessment, the CIT met again to share the results of this and the human resources or security investigation. Usually, the subject was judged to be low or no risk.
6. Interventions & monitoring: EAP would continue to monitor the case for as long as necessary, and there may be interventions including referrals for counselling.

Resources used in threat assessment

In investigative stages, facts were ascertained from supervisors, managers, and EAP assessments.

Risk assessment instruments used
Mental health practitioners used psychological tests during their evaluation, including the MMPI and TAT.

Remote vs. in person threat assessment
Before referring for a mental health evaluation, the EAP professional often completed an in person assessment first. For the psychological evaluation, it was more helpful when there was an interview along with psychological tests.

Threat assessment output
Main outputs were a decision on whether the subject posed a risk, and a resulting management plan.

Interventions

In-house interventions
There were no in-house interventions, beyond exclusion from the worksite.

Outsourced interventions
EAP often made referrals to counsellors in community mental health agencies.

Case management structure

EAP would monitor the case for as long as necessary.

Quality/standards assurance

Data collection and record keeping practices
One of the main principles of the People Team was documenting everything carefully. For the CIT, EAP files were kept separately to personnel files. EAP and psychological assessments were kept only in the confidential EAP file.

Data sharing between agencies
A main principle was confidentiality and discretion. When someone was referred for counselling, there was a release of information so that the EAP professional could be in contact with the mental health provider about the case.

Navy Criminal Investigative Service Threat Management Unit

Summary
The US Navy Criminal Investigative Service (NCIS) Threat Management Unit (TMU) involves a headquarters team and field-based volunteer agents who provide threat assessment consultation to field office teams to prevent workplace violence. The TMU incorporates an operational psychologist to develop recommendations to the subject of interest's command for management.

Threat assessment set up

Background and objectives
The TMU model involves behavioural risk assessment, where the focus is not on profiling violent people, but situations where a person might exhibit violent behaviour (Van Horn, 2013). The aim is to place people at a given time on a continuum of potential for violence. In contrast to traditional law enforcement, the focus is not on making arrests but intervening before a crime occurs to reduce crime and save investigative resources. Communication is a key principle of this model; with other agents, departments (e.g., medical), and people (e.g., victims and witnesses). This is all to prevent violence in an organisation that has unique challenges of access to weapons, young age, stress of deployment, and separation from family.

Threat
The unit targets workplace violence, stalking, school violence, insider threats, high risk domestic violence, rape, arson, and murder for hire, by any person in the Department of the Navy. Most that are investigated are domestic violence, workplace violence, and school violence.

Basic information
- Country: United States
- Setting: Military
- Date of formation: TMU formed in 1994
- Remit: Global

Other involvements
The TMU also supports some counterterrorism and counter-intelligence investigations due to similarities in warning behaviours.

Team details

Specialist vs. multidisciplinary
Multidisciplinary: work is mostly carried out by special agents and investigators, but there is an operational psychologist in the full-time headquarters team.

Team structure
The TMU role overall is to advise on investigative strategies such as people to interview, questions to ask, and information to gather. The TMU comprises a headquarters team that oversees and reviews all investigations and provides guidance to field agents, while the team operational psychologist consults on any significant or complex case. The TMU also has

volunteer field agents who are not necessarily the lead in an investigation in their region, but act as expert consultants helping their field offices with threat assessment and management. The HQ team communicates with the TMU community over email, where anyone can raise an issue with all members, to provide support when trained TMU agents are out of office.

Core team

In the full time TMU headquarters (HQ) team, there are only 4 people:

- Division chief who oversees the TMU
- Operational psychologist who consults on cases
- Two special agents based in TMU headquarters who each cover half of the globe

Additional part time or consulted disciplines

The key aspect of this model is using 30 trained volunteer field agents who already work within navy field offices and take on TMU responsibility voluntarily when they request additional training. At the time of writing, there were 30 such agents.

Training

TMU field agents receive training at least once a year by the HQ team. As they are all already experienced investigators, the training does not cover investigation basics but how to look at a case differently in terms of resources, concerning behaviours, mitigation strategies, interview questions, and case development. This set-up makes the model cost effective; the NCIS only needs to fund annual training of already experienced field agents.

Referrals structure

Case generation

Threats are initially reported to the NCIS by military members, private citizens, or other agencies (e.g., police). The NCIS's Multi-Threat Alert Centre (MTAC) is a monitoring system using hotline numbers, that can contact the NCIS anywhere and anytime. There is also a Text Tip reporting system allowing immediate analysis of anonymous texts from anywhere in the world. Reports can also be made in person, over mail, phone, or email. When the MTAC receives a threat, documented information is passed to the relevant NCIS agent, in this case TMU field agents. TMU field agents in the relevant Navy field office then bring the report to the attention of the TMU HQ team.

Threat assessment operations

Threat assessment process

The TMU process is as follows:

1. Report: threat received by NCIS reporting systems
2. Initial fact finding: the investigating NCIS special agent determines who made the threat, any specific targets, specific wording and method of any threats, how the threat was reported, and whether there were any witnesses.
3. Triage: the investigating team determines whether the threat is predatory (planned, purposeful, and goal-oriented) and high priority. If it is high priority or involving a senior military official, they inform NCIS special agents for protection. If the target is a naval ship, command is notified.

4. TMU consultation: meanwhile, the TMU team take a consultative role in determining the veracity of the threat and next steps, working with the lead of the investigative team. Investigative aims include determining who made the threat, their proximity to the target, civilian involvement, marital or financial issues, relationship with the target, and history of violence or concerning behaviour. They aim to gather as much information as possible both about the facts surrounding the immediate threat, but also background to the subject to give context to the threat, understand motivations, and advise possible future actions.
5. Timeline: the TMU often put this in a timeline of important events, outcomes, and responses to identify any patterns of violence, check facts, provide leads, and potentially support in court.
6. Interrogation: at some stage the subject is interviewed and then released back to their command.
7. Recommendations: the TMU provide a written assessment of findings and recommendations to the NCIS case agent responsible for the investigation and to the subject's command, who then make any relevant investigative decisions and brief any stakeholders.

If the threat is judged to be low risk, there is still a full investigation, but when high risk everything is analysed as high priority and constantly monitored and re-assessed.

Resources used in threat assessment

Various categories of resources are analysed:

- Precise details of the wording and delivery method of the threat or concerning behaviour
- Full biographical data, including Service Record Book of military history if suitable, which contains information on special weapons training and previous disciplinary action
- Open sources: social media and news media, for information on the situation, target, and subject
- Official databases: the National Crime Information Center, Defense Central Index of Investigations, Law Enforcement Information Exchange, and Family Advocacy Program
- US Department of Defense state and local records: for any involvement with any previous investigations and relevance to the current case
- 9/11 tapes or interviews with 9/11 operators: for exact wording of threats and witness information
- Permissive searches of belongings: for weapons, journals, photos, devices etc.
- Documentation of victim injuries if relevant: medical records, photo evidence, all released to investigators with consent of the victim

Remote vs. in person threat assessment

The TMU interview all potential victims and witnesses to determine their perception of why they are targeted, their fear level, any prior threats, and triggers etc. The TMU also recommends that investigators interrogate the subject if they are willing to talk to law enforcement to understand their perspective, target, timeline, plans, and explanations. This is often sufficient to mitigate violence potential.

Threat assessment output
Output of the threat assessment process is an overall report presented to the subject's command, which includes recommendations, timelines, and history.

Interventions

In-house interventions
The TMU team only recommends interventions to the subject's command. Recommendations focus on security and investigative strategies, based on where they are placed on a continuum of potential for violence. If there is a safety concern, they might be referred to medical or recommended a management plan.

Outsourced interventions
It may be recommended that command restrict the subject to their base, monitor the subject, or give a military protective order. TMU often recommends referring the subject for a medical evaluation for risk of violence; NCIS agents cannot themselves refer people, only the command can make referrals. NCIS agents can provide the medical team with their investigative findings. Medical evaluations might result in diagnosis, counselling, or treatment. The TMU can also recommend command to assign someone to conduct welfare checks on the subject so that someone is in constant contact, creating a monitoring system and supporting the subject's wellbeing.

Case management structure
Commands have various potential monitoring systems, including assigning someone to perform welfare checks. The investigation is closed when command has resolved the case, but can be reopened if new information or behaviour arises.

Quality/standards assurance

Data collection and record keeping practices
The reported threat is initially documented in the MTAC. All investigative information is documented in a case file that is given to the subject's command.

Data sharing between agencies
The TMU field agents keep the TMU HQ team continually briefed about progress over email and phone.

Risk Assessment Team at Johns Hopkins University

Summary
This Risk Assessment Team (RATeam) aims to prevent workplace violence in a university. It employs a multidisciplinary team, triage process, extensive information-gathering, and interviews, to provide risk levels and recommendations back to university management for potential interventions.

Threat assessment set up

Background and objectives
This team was implemented through a series of organisational changes in universities in the late 1990s following a student murder in 1996 (Heitt & Tamburo, 2005). Johns Hopkins University set up a multidisciplinary committee that used literature and consultation with experts to produce recommendations for workplace violence prevention. The University then established a workplace violence RATeam.

Threat
The RATeam uses a workplace violence model to account for the range of threats and violence at a university. Initially, a strict threshold limited the RATeam to looking only at cases of assault and battery. The threshold then relaxed to include everything above interpersonal discord. As this proved to be a strain on resources, the threshold was finalised to include antagonism, hostility, intimidation, aggression, harassment, and physical violence.

Basic information
- Country: United States
- Setting: Higher education
- Date of formation: Committee recommendations were implemented and the RATeam established in 1998
- Remit: Employees of the University. Issues related to visitors or patients of the associated medical centre or domestic violence were covered by security a separate taskforce, with some overlap in team membership.

Team details

Specialist vs. multidisciplinary
Multidisciplinary: the RATeam was introduced following recommendations from a multidisciplinary committee on campus violence that had representatives from many university departments including the Employee Assistance Program (EAP), human resources, legal, and security. The RATeam itself is also multidisciplinary, combining expertise and experience from professionals in many disciplines in an interactive and truly collaborative way to form a general understanding.

Team structure
There is a set protocol describing the role of each team member, where each has a set of standardised guidelines to follow for each step, including interviews. The RATeam meets regularly, and separately meets quarterly to review and develop group dynamics.

Core team

The RATeam contains the following disciplines:

- Employee Assistance Program (EAP) or other mental health clinician: who provide a psychological and medical perspective, consultation on behavioural and mental health issues, psychiatric assessment, psychological testing, and forensic risk assessment. They are also the central communication liaison between the whole team, but are not the team leader.
- Security: who provide first response, law enforcement interview techniques and expertise, forensic risk assessment, protective strategies, and follow-up investigations.
- Human resources: who provide guidance on organisational policy, support with the risk assessment process for anyone involved in workplace violence, and initial information-gathering.
- Office of the general counsel: who provide advice surrounding patient safety, relevant legislation, regulatory duties, and risk to property.

Training

In 1999, the RATeam was trained by a professional with experience in workplace violence risk assessment, and this was later repeated to refine and refresh training. All team members received the same training to emphasise the multidisciplinary and equal nature of the team, and to aid with group dynamics. Specifically, clinical staff must be trained in objective and forensic clinical risk assessment, rather than the traditional EAP model of problem assessment.

Referrals structure

Case generation

Threats are reported to one of the RATeam members, who gather preliminary information and then present this to the RATeam by email or conference call if urgent.

Contact with referring bodies

The RATeam experienced problems with reporting processes in a decentralised university due to a lack of designated points of contact. Managers concerned about a certain employee might have contacted junior human resources managers who are insufficiently knowledgeable about the RATeam. The RATeam therefore trained more managers with half day workshops concerning workplace violence and the RATeam reporting process.

Threat assessment operations

Threat assessment process

The RATeam process involves:

1. Reporting: incident or threat is reported to one of the team members.
2. Initial fact finding: the team member who received the report gathers information on the event, relevant people, relationships, and stressors, and writes a detailed report. This is sent to the RATeam by email or conference call if urgent.
3. Triage: RATeam decides whether to conduct a criminal record check, EAP clinical risk evaluation, and human resources or law enforcement investigation. The team decides whether the case is of:
    a. No risk (no action taken), unknown or minor risk: the case proceeds to step 4.

   b. Potential risk (employee potentially taken off duty) or emergent risk (employee is escorted off site by security with their badge, passwords, and keys removed): case is evaluated by all parts of the RATeam. They review all information, evaluate mental health status, and produce a diagnostic formulation and recommendations. These are emailed to the RATeam as agenda points for the next meeting.
4. Discussion in RATeam meeting: the team discuss facts and offer recommendations, including further evaluation by all parts of the team.
5. Recommendations for management
6. Follow-up: with RATeam to monitor intervention results.

Resources used in threat assessment
For their assessment the EAP role uses biopsychosocial history, the Minnesota Multiphasic Personality Inventory-2 (MMPI-2) psychological test, and interviews with managers and witnesses. Further resources used for team assessment include previous problem behaviours, psychiatric history, alcohol or drug use, present and historical familial, marital, and social relationships, medical history, and a mental health evaluation.

Risk assessment instruments used
The EAP member uses MMPI-2: a psychological test used in clinical and non-clinical settings. This is a 567 item self-report measure of a person's psychological state, measuring depression, anxiety, post-traumatic stress, personality characteristics, and general personality traits.

Remote vs. in person threat assessment
Security and EAP conduct interviews as part of their evaluation. EAP interviews can be with management, witnesses, and the subject in a clinical interview. This is supplemented with a personal history questionnaire, which has some overlap to reveal any inconsistencies. All interviews are standardised using questionnaires laid out in the team's protocol.

Threat assessment output
Final output is a presentation of findings and recommendations to management.

Interventions

In-house interventions
There are no in-house interventions beyond human resources supporting the implementation of management recommendations and reporting back to the RATeam.

Outsourced interventions
Recommendations are given to management, which may include termination, disciplinary action, formal referral to EAP, or return to duty with no intervention.

Case management structure

Human resources support implementation of management recommendations and reports back to the RATeam to monitoring outcomes.

Quality/standards assurance

Performance and efficacy evaluations

The RATeam conducts focus groups with managers and others that have been through the process and implement any areas for improvement, and also attempted to develop a measure of outcomes and return on investment.

Data sharing between agencies

The EAP member shares clinical information with the rest of the RATeam when necessary, with the consent of the employee of concern.

United States Postal Service Employee Assistance Program

Summary

Each United States Postal Service (USPS) district has a workplace violence prevention committee, comprising a workplace violence critical incident response team (CIRT) and a threat assessment team (TAT). These are multidisciplinary teams and, through involvement of the Employee Assistance Programme (EAP), have extensive capacity to provide in-house counselling.

Threat assessment set up

Background and objectives

These teams are part of the wider USPS workplace violence prevention program that focuses on multidisciplinary collaboration, early identification of risk before a crisis occurs, comprehensive assessment, prompt intervention with support for employees, and participation at the executive level (Kurutz et al., 1996).

Threat

Workplace violence, involving employees or their families.

Basic information

- Country: United States
- Setting: Commercial organisation
- Date of formation: Programs for workplace violence were established in 1994. This was an expansion on the EAP which was initially set up in 1968 as the Program for Alcohol Recovery, and later expanded to treat other drug dependencies in 1986.
- Remit: USPS employees and their families

Other involvements

The EAP has many roles beyond prevention of workplace violence, including employee wellbeing, absenteeism, disputes, disability claims. They provide a 24-hour helpline, counselling, support for employees with issues including mental health, relationships, drug or alcohol use, gambling, and grief, and training on organisational issues including workplace violence.

Team details

Specialist vs. multidisciplinary

Multidisciplinary: workplace violence prevention committees contain numerous USPS departments.

Core team

Each district's workplace violence prevention committee has:

- EAP coordinator: who do not provide counselling but are on the workplace violence committee, respond to critical incidents, design the committee, are a point of contact for intervention services, provide direct communications to leadership and employees, and handle relations with media and victim families.
- Other EAP roles: EAP professionals work on the CIRT and TAT, alongside many other employee wellbeing roles

- Medical
- Human resources
- Labour relations
- Operations management
- Inspection Service

Referrals structure

Case generation
Cases are generated by a referral concerning an employee or their family member. For the EAP's general non-threat assessment activities, referrals can be from the employee themselves, supervisors, union leaders, medical professionals, or family members.

Contact with referring bodies
The EAP provides training to key workplace contacts including supervisors and union leaders. This is 8-hour training consists of identifying, preventing, and responding to workplace violence, with a focus on early warning signs of troubled employees.

Threat assessment operations

Threat assessment process
The TAT's process is as follows:

1. Assessment of potential risk of violence: using the Threatening Correspondence Program. Evaluation is made considering threats to individuals, organisation threats, current volatility of the worksite, specific plans for violence, and risk indicators of psychiatric disorders, alcohol, or drug abuse.
2. Action plan: the committee develop a risk reduction and threat management plan focusing on respect and dignity of employees, which is reviewed by local and district management.
3. Implementation
4. Follow-up: usually by the human resources manager and EAP coordinator.

Threat assessment output
Main output is a risk reduction strategy and threat management plan.

Interventions

In-house interventions
Any intervention is usually supervised by the human resources manager and EAP coordinator. The EAP is equipped to provide in-house counselling, with hundreds of full-time professionals. All counsellors must have a master's degree, relevant certification, at least three years of experience, and specific training on the USPS organisation.

Outsourced interventions
The EAP may also refer to community resources or affiliate counsellors for accessibility reasons or specific expertise.

Case management structure

The EAP follows up to ensure counselling treatment attendance and progress.

Quality/standards assurance

Performance and efficacy evaluations
Data from the EAP Information System are used to ensure decisions are based on available evidence.

Data collection and record keeping practices
The EAP Information System is a national database input by counsellors of training, client demographics, outcome data, clinical details, and consumer satisfaction information. This became available nationwide in 1995.

Fixated Threats and Protection of Public Officials

Los Angeles Police Department Threat Management Unit

Summary

The Los Angeles Police Department (LAPD) Threat Management Unit (TMU) is a specialised police unit that started as a liaison for the entertainment industry and now assesses a wide range of threats. As a police unit, the TMU has extensive capabilities for information-gathering and interventions.

Threat assessment set up

Background and objectives

The LAPD established the TMU following the murder of actress Rebecca Schaeffer (Bixler et al., 2021; Dunn, 2013). At the time there were no anti-stalking laws or ways to report stalking to law enforcement without a criminal offence. The case raised awareness of the need for early detection, intervention, and case management, as well as the presence of mental illness and problematic communications preceding attacks (Bixler et al., 2021; Dunn, 2008; 2013). The TMU was started as multidisciplinary collaboration between the LAPD and entertainment industry, as a point of contact for the entertainment industry to report obsessive but not necessarily criminal behaviours (Bixler et al., 2021; Dunn, 2008; 2013).

Threat

Targeted threats primarily include stalking and other long-term obsessive behaviours, workplace violence of city employees, and threats to public figures (e.g., celebrities and politicians) (Bixler et al., 2021; Dunn, 2008; 2013).

Basic information

- Country: United States
- Setting: Law enforcement
- Date of formation: 1990
- Remit: Citywide

Other involvements

The TMU also staffs other threat assessment teams within Los Angeles, and co-hosts the annual National Threat Management Conference (Dunn, 2008; 2013).

Team details

Specialist vs. multidisciplinary

The TMU is a specialist police unit, though it is placed within the LAPD's Mental Evaluation Unit which involves mental health crisis response (Bixler et al., 2021). It was created as a multidisciplinary collaboration between law enforcement and the entertainment industry, but this collaboration is primarily to encourage referrals rather than facilitate assessment (Dunn, 2008; 2013).

Team structure

The core team is all police officers, usually comprising several detectives and one officer in charge, who ensures the team has the resources and time for the caseload (Bixler et al.,

2021; Dunn, 2013). There are regular team meetings to keep this supervisor informed and all officers aware of all live cases.

Training
All team members have a minimum of 15 years of law enforcement experience. Due to the caseload involving interacting with traumatised people and complex case management, their experience must include working on domestic violence cases, sexual assault investigations, and computer forensics (Bixler et al., 2021; Dunn, 2013). All LAPD officers also have 40-hour mental health intervention training (Bixler et al., 2021).

Referrals structure

Case generation
Cases can be referred to the TMU from (Bixler et al., 2021; Dunn, 2013):

- The public, including victims or private security professionals. These cases are initially screened over the phone.
- Entertainment studios and staff in offices of elected officials, for fixated threats.
- Prosecutors requiring assistance on a case given to them by another investigator.
- Los Angeles city department and City Threat Assessment Team, for workplace violence cases.
- Major Assault Crimes units, who are frequent referrers due to heavy caseloads, so there are criteria for the TMU accepting cases.

Initial threats that are reported include phone calls, emails, trespassing, identity theft, internet activity, and vandalism (Dunn, 2008).

Contact with referring bodies
The TMU acts as a liaison contact for other agencies including entertainment industry security, elected officials, the FBI Behavioral Analysis Unit, US Capitol Police, US Secret Service, CIA, and Navy Criminal Investigative Service (Bixler et al., 2021; Dunn, 2008; 2013). To help detect patterns and escalation in cases involving public figures, management offices often designate one person to keep a log of all contact from the suspect (Dunn, 2008).

Threat assessment operations

Threat assessment process

1. Triage: for example, the LAPD MEU has a triage desk to identify threats and refer them to the TMU (Bixler et al., 2021), and cases from the Major Assault Crimes unit are screened over the phone for certain criteria (Bixler et al., 2021). More generally, LAPD responding officers to stalking situations ask probing questions to help with case prioritisation for threat assessment (Dunn, 2008).
2. TMU interview of victim (Bixler et al., 2021; Dunn, 2008; 2013).
3. Gathering of evidence and statements (Dunn, 2008).
4. Threat assessment: a brief initial assessment due to limited information and time, involving methods of contact, context, relationship between target and suspect, and history of violence. This is adapted as more information is received (Bixler et al., 2021; Dunn, 2008; 2013).
5. Case management: with a focus on victim safety and approval. Case management strategies differ case by case depending on the proximity of the suspect, nature of

contact, seriousness of the threat, and volume of evidence to prosecute (Bixler et al., 2021; Dunn, 2008; 2013).

Resources used in threat assessment

In the evidence gathering stage, the TMU collects phone records, voicemails, emails, computers, belongings, internet history, photos of any injuries or property damage, medical records, and witness interviews (Dunn, 2008; 2013). Search warrants and subpoenas are crucial for phone companies, internet service providers, and financial institutions (Dunn, 2008). The TMU has developed custom templates of search warrants and subpoenas to speed up information-gathering (Bixler et al., 2021). Information considered in threat assessment includes the suspect's criminal history mental and physical health, living situation, finances, relationship with the target, and support system (Bixler et al., 2021; Dunn, 2008; 2013). Cyber elements are increasingly important in assessing stalking threats, including through examining emails, blogs, and activities in internet cafes and public libraries (Dunn, 2008).

Remote vs. in person threat assessment

The TMU interviews the victim to gather information on the nature and context of the threat, and their relationship with the suspect. The interview is also to build rapport, and inform them about the investigation process, protection opportunities, and their limits (Bixler et al., 2021; Dunn, 2008; 2013). This often takes several hours and follows an interview by the initial LAPD responding officer (Bixler et al., 2021; Dunn, 2008; 2013). The TMU always re-interviews witnesses and victims in this way as duty and patrol officers are not trained on probing for relevant information (Bixler et al., 2021; Dunn, 2013).

Threat assessment output

The main output from the threat assessment process is case management and intervention strategies.

Interventions

In-house interventions

As a police unit, the TMU has in-house intervention capabilities. These can include security recommendations for the victim, verbal warnings to the suspect, restraining orders, involuntary mental health detention and psychiatric evaluations, arrest, and prosecution (Bixler et al., 2021; Dunn, 2008; 2013).

Outsourced interventions

Many of the in-house intervention possibilities are routes to other interventions or treatment (Bixler et al., 2021; Dunn, 2008; 2013): restraining orders can facilitate arrest if they are violated; involuntary detention can involve treatment for mental health issues, welfare checks, and prohibitions on firearms possession; and prosecution might lead to anger management training and electronic monitoring.

Quality/standards assurance

Performance and efficacy evaluations

The TMU has struggled to quantify its effectiveness due to its aim of intervention before violence occurs, but it is confident it has saved lives and also financial liabilities in workplace violence cases (Bixler et al., 2021).

Data collection and record keeping practices

All cases are documented, including any threat assessments, interventions, and follow-ups (Bixler et al., 2021).

Data sharing between agencies

Some privacy laws restrict hospitals sharing treatment or diagnosis information with the LAPD. Often more important for threat assessment is the reverse, as police can share information with physicians to aid treatment and diagnosis (Bixler et al., 2021).

Mental Health Liaison Program, consulting to the United States Secret Service

Summary
The Mental Health Liaison Program (MHLP) comprises psychiatric and psychological professionals who consult to the United State Secret Service (USSS) teams on threats to leaders and dignitaries, altogether creating a multidisciplinary approach. The MHLP's main roles include case consultation, training, and liaison, and do not include treatment.

Threat assessment set up

Background and objectives
One of the USSS's main roles is to protect leaders and dignitaries. Beyond physical protective security, this now includes threat assessment and protective intelligence (Phillips, 2008), involving identifying, investigating, assessing, and managing people who might pose a threat (Coggins & Pynchon, 1998). The USSS's relationship with mental health services began after Institute of Medicine recommendations on case consultation by mental health agencies, following conferences with experts (Phillips, 2008). There is a clear role of mental health in people that are referred to the USSS and attempt assassinations; however, most do not meet the criteria for civil commitment and lack social support services, so need a case management agency for evaluation and treatment. The MHLP supports these objectives through its roles of 1) case consultation, 2) training, and 3) liaison.

Threat
Assassinations and threats to public figures, including fixated threats (Coggins & Pynchon, 1998).

Basic information
- Country: United States
- Setting: Law enforcement
- Date of formation: MHLP was created in the late 1980s, in an attempt by the USSS following the Institute of Medicine report to formalise the relationship with mental health agencies and expand this nationwide (Coggins & Pynchon, 1998).
- Remit: Nationwide

Other involvements
The MHLP often works with consultants and behavioural researchers to present papers at academic conferences (Coggins & Pynchon, 1998). They also provide extensive training and consultation to the USSS on mental health issues related to the USSS beyond threat assessment, including evaluation and diagnosis, interviewing the mentally ill, mental health services, confidentiality, regulations surrounding civil commitment, and other ethical and legal aspects of the relationship between law enforcement and mental health services (Phillips, 2008).

Team details

Specialist vs. multidisciplinary
Multidisciplinary: the initial driver behind the MHLP was a push towards law enforcement and mental health service collaboration in the 1980s (Coggins & Pynchon, 1998). The aim of the MHLP is to pair psychiatric and psychological consultants with USSS field offices to

consult on risk assessment or case management, train agents in mental health issues, and act as a liaison between the USSS and the mental health community (Coggins & Pynchon, 1998). This has helped to bridge boundaries and improve communication between law enforcement, mental health, social, and criminal justice systems, and helped agents gain awareness of the relevance of mental health in evaluation and management of subjects. While the MHLP itself only comprises psychiatric and psychological consultants, the overall approach is multidisciplinary (Phillips, 2008).

Team structure

USSS case agents have responsibility for directing cases, collecting information, making risk judgements, and implementing case management, while MHLP consultants help agents to manage and evaluate these cases (Coggins & Pynchon, 1998; Phillips, 2008).

Core team

The full-time MHLP team are psychiatric and psychological consultants, who consult to USSS case agents. The lead of the team is the case agent who makes final decisions (Coggins & Pynchon, 1998).

Training

A fundamental role of the MHLP is providing training to USSS agents who ordinarily have no experience in clinical risk assessment or mental health services but consult the MHLP for this service (Coggins & Pynchon, 1998). MHLP consultants provide professional development training to new agents as basic training, and more intensive courses when agents assume responsibility within protective intelligence. Training includes risk assessment principles, interviewing the mentally ill, and pharmacological treatments in the form of role-play scenarios, case studies, and simulations of multidisciplinary working. Agents have reported on the benefits of this training regarding confidence handling their caseload, better communication between agencies, and appreciation for the role of mental health.

Referrals structure

Case generation

USSS agents have discretion over requesting consultation from the MHLP, and have direct access to the regional MHLP consultant to do so (Coggins & Pynchon, 1998).

Contact with referring bodies

If unsure about referring a case, USSS agents can discuss with a consultant without starting a formal case review (Coggins & Pynchon, 1998). Guidelines state that the MHLP consultants should be contacted if agents are inclined to classify a threat as high risk and needing intensive case management, or when a case is about to be closed, to check on dynamic risk factors.

Threat assessment operations

Threat assessment process

For the USSS case agents, the threat assessment process is (Phillips, 2008):

1. Identification: of individual posing a threat.
2. Investigation.

3. Assessment: of whether they pose a risk.
4. Development and implementation of management plan: if there is a risk of danger.

Within this, the MHLP consults on these cases to aid in comprehensive risk assessment, and their process involves (Coggins & Pynchon, 1998):

1. Initial assessment: before MHLP involvement, the USSS case agent has already analysed the concerning behaviour, conducted an interview, and looked at mental health and criminal history.
2. Case consultation request: the request to the MHLP could be a basic question, such as the side effects of a medication, or more complex such as help developing a risk management plan. Usually, they request support assessing risk of harming a protected official, or case management help to secure resources for medical, psychiatric, or social needs.
3. Case consultation: MHLP consultants analyse available information and conduct interviews to clarify what mental health factors are relevant, review previous evaluations, develop hypotheses about likelihood for concerning behaviour in the future, suggest investigative strategies to evaluate risk level, and advise on treatment.
    a. Liaison: the MHLP also establishes liaison between the USSS and local mental health services to help access information or find resources for interventions.
4. Report: the MHLP produces a report, submitted to the USSS and included in their casefile.

Resources used in threat assessment

The MHLP consultant is one resource itself, used by the USSS when assessing risk and threats. Resources looked at in case consultation are case materials already prepared by the agent, including interviews with the case manager, investigative reports, previous forensic evaluations, psychometric information, mental health history, criminal history, and prior involvement with the USSS (Coggins & Pynchon, 1998; Phillips, 2008). The consultant might also interview the subject of concern and liaise with treatment professionals.

Remote vs. in person threat assessment

Before MHLP involvement, the subject is interviewed by the case agent, and this may be followed up by another interview and psychiatric evaluation with the MHLP consultant (Coggins & Pynchon, 1998; Phillips, 2008). The consultants delay interviewing the subject until any criminal matters have first been resolved (Coggins & Pynchon, 1998).

Threat assessment output

The written report from the MHLP depends on the initial reason for referral, but usually will include recommendations for strategies to gain more risk assessment information (Coggins & Pynchon, 1998). The final output from the threat assessment process is the USSS agent's judged level of risk and management plan, as they have decision-making power (Phillips, 2008).

Interventions

In-house interventions

The MHLP do not carry out in-house interventions and must clarify with subjects during interviews psychiatric evaluations that they are not present in a treatment capacity (Coggins & Pynchon, 1998).

Outsourced interventions

The third main role of the MHLP is liaison activities (Coggins & Pynchon, 1998). They create networks between field offices and local facilities that can provide treatment, often by creating forums through conferences. They also provide training to mental health facilities on the USSS protective intelligence programme.

Case management structure

The MHLP reviews cases to ensure that mental health and social support services are available when required (Coggins & Pynchon, 1998).

Quality/standards assurance

Performance and efficacy evaluations

The MHLP has annual evaluations using input from consultants, USSS offices, and agents (Coggins & Pynchon, 1998). Additionally, they have at least biennial program evaluation conferences to review activities, research findings, and specific cases. While there is no empirical data on the liaison role, USSS feedback suggests most problems occur in situations where there is no established liaison, and the permanent MHLP was created from positive feedback following a three-year pilot liaison program with five field offices. The MHLP are eager for evaluation research into their activities, client satisfaction, and effectiveness, and into any gaps in understanding of mental health systems in law enforcement.

Data collection and record keeping practices

The MHLP report is kept in the USSS casefile (Phillips, 2008).

Data sharing between agencies

According to MHLP guidelines, direct contact between consultants and subjects or treatment teams must start with disclosure about the consultant role and relationship with the USSS, that they are not present in treatment capacity, and that there is no therapist-patient privilege (Coggins & Pynchon, 1998). The case agent must always be present.

United States Capitol Police Threat Assessment Section

Summary
The United States Capitol Police (USCP) has a Threat Assessment Section (TAS) to assess and respond to all threats to members of Congress. The team use triage to save resources for complex cases, and use procedures and risk assessment tools borne out of empirical research through a university collaboration.

Threat assessment set up

Background and objectives
TAS operations are based on research, due to an ongoing collaboration with Mario Scalora's university research team (Scalora et al., 2008). This has produced an empirically evidenced set of risk factors that focus not only on immediate factors and details surrounding the concerning behaviour or threatening communication, but also the background and context to both the threat and the threatener.

Threat
Threats against members of Congress.

Basic information
- Country: United States
- Setting: Law enforcement
- Date of formation: USCP TAS was set up in 1986.

Referrals structure

Case generation
Cases come to the USCP TAS by referral. This usually begins when the subject attempts to contact a member of Congress through letters, calls, emails, packages, or physical approach. These are received by the state or district offices or by the Capitol Hill office.

Threat assessment operations

Threat assessment process
Before threat assessment begins, there is an initial triage to determine risk factors and the extent of the investigation and threat assessment.

Risk assessment instruments used
The TAS uses risk factors from professional established risk assessment instruments and from academic work from collaborations between Scalora's university research group and TAS research. These empirically backed risk factors concern the contact behaviour, the individual's background, and contextual factors. These factors overall are categorised into contextual, subject, motivational, target, protective, and contact behaviour.

Quality/standards assurance

Performance and efficacy evaluations

The TAS partnership with Scalora's university group allows for empirical research and program evaluation. There is constant re-evaluation of their risk factors for predictive validity to ensure they are empirically supported. There is also analysis of patterns in concerning behaviours that come to the TAS. This helps identify and anticipate emerging trends such as cyber threats, biochemical threats, and increasing numbers of subjects with mental illness.

Data collection and record keeping practices
All communications and incidents that are referred are documented, at minimum.

Fixated Threat Assessment Centre

Summary
The Fixated Threat Assessment Centre (FTAC) is a fully multidisciplinary unit comprising healthcare and police staff that assesses fixated threats and lone actor grievance-fuelled violence. Threat assessment triage can be followed by more nuanced risk assessment, and interventions comprise FTAC making recommendations and developing networks of services around a subject to catalyse a joint multi-agency response.

Threat assessment set up

Background and objectives
FTAC was developed following the Fixated Research Group's findings that many problematic approaches and behaviours were driven by a treatable mental illness, and individuals exhibited pre-attack warning behaviours including communications and threats (Wilson et al., 2021). There was therefore a fundamental role for psychiatry in the protection of public figures (James et al., 2013). FTAC follows a public health model, where the risk factor being treated is unmet mental health needs (Barry-Walsh et al., 2020; James et al., 2013; Wilson et al., 2021). The main aim is not to predict violence but to intervene to reduce risk and prevent harm (Barry-Walsh et al., 2020). Interventions aim to reduce the risk of harm to both the target (including psychological distress and practical disruption) and to the mental and legal wellbeing of people referred (Barry-Walsh et al., 2020). They are diverted towards services that have not yet treated or identified them, often because they do not have serious mental illnesses (James et al., 2013; MacKenzie & James, 2011).

Threat
Lone actor stalking of, harassment of, and threats to public figures, primarily the Royal Family and politicians (James et al., 2013). This also includes threats to relevant sites including palaces and parliament buildings.

Recently, this model has also considered lone actor grievance-fuelled violence, given the overlap with fixated threats in presence of mental illness and leakage behaviours (Wilson et al., 2021). In 2016-2017 London psychological staff from FTAC began working with counterterrorism police to counter radicalisation (Barry-Walsh et al., 2020). This created a new unit where individuals could be referred to FTAC for mental illness under Prevent.

Basic information
- Country: United Kingdom
- Setting: Law enforcement
- Date of formation: FTAC was formed in 2006, initially as a pilot scheme for 18 months. This was borne out of the empirical importance of mental illness evidence in the Fixated Research Group work, which commenced in 2003 (Barry-Walsh et al., 2020; Wilson et al., 2021).
- Remit: Nationwide, based in London
- Funding source: Joint funding from the Department of Health and the Home Office's Office of Security and Counterterrorism (Barry-Walsh et al., 2020; James et al., 2013)
- Team location: Metropolitan Police, in central London

Other involvements

FTAC is also involved in (Wilson et al., 2021):

- Consultation and education for other agencies regarding referral processes, often for difficult cases that do not involve public figures (James et al., 2013).
- Security planning regarding fixated threats for major events, nationally and internationally (Barry-Walsh et al., 2020). It also has staff in operational control rooms for these events.
- Research to improve risk assessment instruments, resulting in the development of the CTAP-25 (Barry-Walsh et al., 2020).
- Delivering briefing materials when dignitaries are planning security for travel (James et al., 2013).
- Formal reviews of threat levels to people under personal protection.
- Setting up the European Network of Public Figure Threat Assessment Agencies, with an annual conference.

Team details

Specialist vs. multidisciplinary

Multidisciplinary. FTAC is fully integrative, as it is a police unit but staffed by both police and healthcare professionals, with all cases jointly processed and signed off (Wilson et al., 2021). The presence of psychiatric professionals helps to understand mental health and motivations, gain diagnoses, and catalyse appropriate sources for interventions (Barry-Walsh et al., 2020; James et al., 2013; MacKenzie & James, 2011; Wilson et al., 2021). To prevent and mitigate stalking-related violence, a large combination of processes (assessment, support, interventions, treatment, and management) and disciplines (legal, psychological, law enforcement) are required (MacKenzie & James, 2011). A central part of FTAC is forming networks of agencies through the whole process to enable referrals, information-gathering, interviews, interventions, and management (James et al., 2013).

Team structure

There are three caseworker teams comprising one forensic nurse or social worker and two detective constables each. A senior psychologist manages the risk assessment process and a detective sergeant manages police staff (James et al., 2013; Wilson et al., 2021).

Core team

The core team is staffed by police and mental healthcare professionals, led by a detective chief inspector, (James et al., 2013; Wilson et al., 2021). In total, there are nine police officers and four full time forensic nurse specialists (James et al., 2013; Wilson et al., 2021).

Additional part time or consulted disciplines

Part time staff include three consultant forensic psychiatrists and one consultant psychologist (James et al., 2013; Wilson et al., 2021).

Training

All mental health professionals in the team are trained in the Stalking Risk Profile (MacKenzie & James, 2011).

Referrals structure

Case generation

Cases are identified both by proactive searches and referrals. Searches include daily checks of police intelligence systems for anything within FTAC's remit, and an emerging strategy to search online social media content (James et al., 2013). Referrals follow a subject making a concerning communication or approach, in the form of a letter, poster, lawsuit, or leakage (Wilson et al., 2021). Reports come to FTAC mostly over phone and email from protective personnel, communication offices, or office staff, accompanied by an email with attachments of the initial concerning communication (James et al., 2013). Reports occasionally come from counterterrorism police, who might hand the entire case over if mental illness is thought to be the leading factor (Barry-Walsh et al., 2020).

Contact with referring bodies

FTAC gives communications offices checklists to use as a screening tool for who should be referred. This is audited by FTAC in light of research findings and evaluations of false negatives and positives from previous referrals (James et al., 2013; Wilson et al., 2021). Each referring agency has a designated FTAC contact who gives training and feedback on case outcomes. This training is important due to high staff turnover in these offices. FTAC also provides talks and information to those responsible for physical building protection, MPs, and their staff (James et al., 2013).

Threat assessment operations

Threat assessment process

The FTAC process involves:

1. Referral from agency.
2. Information-gathering: immediately, within a few hours of when a threat is referred (James et al., 2013).
3. Threat assessment: involving discussions between the case's nurse and detective, supplemented by an aide memoire. This results in a level of concern, on the day the referral is received (James et al., 2013). This is signed off by the detective sergeant and consultant forensic psychiatrist.
    a. If low level of concern, this is reported back to the referrer, to save FTAC and other police resources (James et al., 2013).
    b. If medium or high level of concern, the case proceeds to a management plan.
4. Management plan: throughout the process, there is a focus on the risk factors that can be intervened with and managed (James et al., 2013; Wilson et al., 2021).
5. Further action: from here, there may be an immediate short- or long-term intervention, or more information-gathering and nuanced risk assessment (James et al., 2013; Wilson et al., 2021). This may include seeking information from other sources (e.g., healthcare) and building a network of support systems around the subject (Wilson et al., 2021). This continues until the cases is of low concern.
6. Risk assessment: using further information gathered.
7. Interventions and case management.
8. Case closure or follow-up (Wilson et al., 2021).

Resources used in threat assessment

In information-gathering stages, the detective and nurse use police databases and systems, previous correspondence between the subject public figures, firearms registers, and internet searches (Barry-Walsh et al., 2020; James et al., 2013). They also discuss with and gather information from the subject's GP and the referrer of the threat, though health information is only sought if more nuanced risk assessment is required at steps 5-6 (Wilson et al., 2021).

Risk assessment instruments used

In the threat assessment period, the CTAP is used to judge the level of concern (Wilson et al., 2021). The CTAP was created from FTAC research, and operates as both a screening and threat assessment tool to determine the urgency of an intervention through assessing the content of communications (Barry-Walsh et al., 2020; Wilson et al., 2021). The aide memoire used in initial information-gathering has 38 risk factors, many of which are psychological so require expertise of mental health professional on the team (James et al., 2013).

In the risk assessment for medium and high concern cases, SPJ tools are used. In particular, FTAC use the computerised SRP for public figures, which is categorised into risk of escalation, disruption to the target, persistence, psychological damage to the subject, and violence (James et al., 2013; Wilson et al., 2021).

Remote vs. in person threat assessment

Caseworkers often conduct in person interviews, sometimes at the subject's home or during an approach, which require risk assessments for staff safety (James et al., 2013). Interviews regarding complex cases are often joined by the consultant psychiatrist or psychologist (Wilson et al., 2021). This allows detailed reports to be passed to psychiatric services (Wilson et al., 2021).

Threat assessment output

The main output is a level of concern in the threat assessment stage, and a management plan to mitigate this concern, which is dynamic and constantly revised (Barry-Walsh et al., 2020; James et al., 2013). Concern levels are preferable to risk levels, given there is limited information and time to make the decision (Barry-Walsh et al., 2020).

Interventions

In-house interventions

FTAC does not perform any in-house interventions, criminal investigations, or psychiatric treatment themselves, beyond warning potential targets of threats. Their role is to form a network of services around the subject, recommend strategies to these services, catalase a multi-agency response, and then provide follow-up. (James et al., 2013; MacKenzie & James, 2011; Wilson et al., 2021). Here, FTAC's relationship with mental health agencies is invaluable; services are more likely to respect and value referrals from other psychiatrists than police agencies (James et al., 2013).

Outsourced interventions

Referrals can be made to many agencies including social services, housing, family agencies, police, and mental health services, and can have long- or short-term suggestions (Barry-Walsh et al., 2020; Wilson et al., 2021). Police interventions can include revoking gun

licenses, target protection, a check on the target's home by local police, or contact with community police officers (James et al., 2013). Mental health interventions can include referral to local agencies, providing more information, or suggesting treatment. Most serious interventions, including pressing criminal charges or detaining a subject under the Mental Health Act, ensure that the subject gets resources from healthcare services. Psychiatric services in particular see FTAC patients as very different to their traditional clientele, so FTAC, beyond arranging liaison networks of agencies, also is an expert consultant to advise on evaluating and managing fixated individuals (MacKenzie & James, 2011).

Case management structure

FTAC does provide follow-up, with an understanding that most cases cannot be solved by short term treatment or solutions, and require extensive case management (James et al., 2013). The multi-agency response allows updates on intervention effectiveness from local services who are in contact with the subject (Wilson et al., 2021). There are weekly case reviews once cases are at a sufficiently low level of risk with a stable management plan, and then quarterly reviews (James et al., 2013).

Quality/standards assurance

Performance and efficacy evaluations

FTAC uses satisfaction surveys, risk factor audits based on casework, efficacy evaluations, and program evaluations (James et al., 2013). There has also been follow-up looking at cases two years and one year either side of an intervention to see changes in communication patterns (Wilson et al., 2021).

Data collection and record keeping practices

Documentation follows standardised protocols and is recorded on a computerised database. This ensures all the same information is gathered from each case, allows insights on case progression, ensures assessments are completed the same way, and means information on risk factors is always ready to be analysed (James et al., 2013).

Data sharing between agencies

One of FTAC's main purposes is to share information between agencies to catalyse interventions, which is often restricted by regulations (Barry-Walsh et al., 2020). Even within FTAC, there are limitations to sharing medical information from nurses with police unless there is a serious risk to harm, which is often fulfilled in FTAC's cases (James et al., 2013; Wilson et al., 2021). More often, it is police information being shared with psychiatric professionals that is more important, so they are fully aware of the content and context of threatening communications.

Queensland Fixated Threat Assessment Centre

Summary
The Queensland Fixated Threat Assessment Centre (QFTAC) is a multidisciplinary unit of police and mental health professionals. It was originally designed to target threats against public figures, but has now expanded into lone actor grievance-fuelled violence where there is a clear mental health concern. The QFTAC model centres on facilitating intervention and treatment through a multi-agency response.

Threat assessment set up

Background and objectives
QFTAC followed the UK FTAC model of applying a joint police and mental health unit to mitigate fixated threats, given the prevalence of mental illness (Pathé et al., 2018). The goal is not to predict violence but prioritise the urgency and determine the level of intervention and monitoring. QFTAC operates by a public health model, targeting interventions towards high-risk groups. Several other units in Australia operate on a similar model, including: the New South Wales Fixated Persons Intervention Unit, FTACs in Victoria, Western Australia, and smaller jurisdictions, and an Australian Federal Police (AFP) FTAC in Canberra.

Threat
Initially, QFTAC and similar Australian models focused only on fixated threats to public figures involving problematic approaches or communications and untreated mental illness (Pathé et al., 2018). This was expanded in 2016, through Project Solus, to include lone actor grievance-fuelled violence given the commonalities with fixated threats: personal grievances, perceived injustices, mental illness, and leakage (Pathé et al., 2018; Wilson et al., 2021). These factors mean attacks could be preventable with a multi-agency response. All Australian FTAC models include this new threat, except the AFP FTAC in Canberra, which remains focused on fixated threats to politicians.

Basic information
- Country: Australia
- Setting: Law enforcement.
- Date of formation: QFTAC was set up in 2013 (Barry-Walsh et al., 2020) and expanded to include lone actor grievance-fuelled violence in 2016 (Wilson et al., 2021).
- Remit: State-wide, covering any security person of interest with a current or historic mental illness (Pathé et al., 2018; Wilson et al., 2021).

Other involvements
QFTAC also helps in investigations into lone actor grievance-fuelled violence, primarily in assessment and public messaging (Pathé et al., 2018), and is involved in security for major events (Wilson et al., 2021). These Australian FTACs also help provide training to police and mental health agencies in all jurisdictions about assessing lone actor grievance-fuelled violence.

Team details

Specialist vs. multidisciplinary
QFTAC is fully multidisciplinary and jointly staffed by both police and mental health personnel, recognising that only a multi-agency approach can address extremism threats (Pathé et al., 2018; Wilson et al., 2021). Mental health professionals in QFTAC have helped counterterrorism investigators and intelligence officers coordinate management with better awareness on complex mental health issues (Pathé et al., 2018).

Team structure
Each case is seen by a police and mental health caseworker team, and there are weekly multidisciplinary case management meetings (Pathé et al.).

Core team
Australian FTAC models are police units but incorporate psychiatric personnel (Wilson et al., 2021).

Additional part time or consulted disciplines
The Victoria FTAC also has intelligence officers and analysts to examine electronic footprints (Wilson et al., 2021).

Referrals structure

Case generation
Cases come to QFTAC by referral from counterterrorism organisations, mental health services, the public, public offices, and any agency in contact with vulnerable people (including law enforcement, intelligence, youth justice, family violence, educational, adult mental health, and correctional services) (Pathé et al., 2018; Wilson et al., 2021). Project Solus cases often are referred through the Australian National Security Hotline which provides a 24-hour phone line for the public to resort suspicious behaviour, travel, or social media activity (Pathé et al., 2018). Cases are then triaged by the Tri-Agency Security Intelligence Group before being taken to QFTAC for mental health expertise. The counterterrorism investigation continues unless it is found that mental health is the major concern.

Contact with referring bodies
QFTAC trains stakeholders who refer to them in identifying cases, what to refer, and how to refer (Pathé et al., 2018; Wilson et al., 2021). For fixated persons cases, constituency offices and judicial staff are given an empirical checklist of risk factors to screen which cases to pass on to QFTAC (Pathé et al., 2018). For Project Solus, referrers are given a tool to screen for the presence of psychopathology, in which case it should be referred to QFTAC. If there is some mental disturbance but not mental illness, these should still be discussed with an QFTAC clinician.

Threat assessment operations

Threat assessment process
For fixated threat cases:

1. Initial screening: by referring stakeholders using empirical checklist of risk factors to determine what to pass to QFTAC (Pathé et al., 2018).
2. QFTAC involvement: the case is given to a joint mental health and police caseworker team (Pathé et al., 2018).
3. Threat assessment triage: to determine a level of concern (Wilson et al., 2021).
    a. If low concern, no action is taken.
    b. If moderate or high concern, QFTAC develops a management plan.
4. Management plan: including interventions and risk assessments using SPJ tools until the case is reduced to low concern (Wilson et al., 2021).

For Project Solus cases:

1. Initial screening: referring stakeholders screen for psychopathology (Pathé et al., 2018). QFTAC are not interested in diagnosis but in behaviour and risk level, meaning they take cases not seen by mainstream mental health services, including personality disorders, acquired brain injuries, autism spectrum disorder, and drug induced psychosis (Pathé et al., 2018; Wilson et al., 2021).
2. Initial assessment: of these persons of interest with possible mental health issues (Pathé et al., 2018).
3. QFTAC caseworker team: cases are looked at by a team of a clinician, constable, and analyst (Wilson et al., 2021).
4. Threat assessment using Risk Aide-Mémoire: the joint team use this to develop a level of concern, with senior staff supervising (Pathé et al., 2018). This is re-administered if there is a change in circumstance, or just before the case is closed to QFTAC.
    a. Low concern: case is not taken on by QFTAC but they may give advice for monitoring back to the referrer (Wilson et al., 2021).
    b. Medium or high concern: requires a management plan. High concern cases require an urgent response.
5. Intervention and management plan: depending on whether the case is decided to be of mental health need, police need, or both (Pathé et al., 2018). The case remains open until reduced to low concern.

Risk assessment instruments used

For fixated threats, QFTAC uses the CTAP-25 to assess the content of concerning communications (Wilson et al., 2021).

For Project Solus, it is hard to find an evidence-based tool with predictive value for terrorism and extremism (Pathé et al., 2018). The focus is instead on prioritising the urgency and level of intervention or monitoring. QFTAC uses a Risk Aide-Mémoire which draws upon literature to reach a level of concern rather than risk, given current and limited information. Items on this list include motivations, mental health status, previous behaviour, and risk factors for radicalisation.

Threat assessment output

The output of the threat assessment process is low, moderate, or high level of concern (Pathé et al., 2018; Wilson et al., 2021). For Project Solus, cases are also categorised into being of mental health need, police need, or both (Pathé et al., 2018).

Interventions

Outsourced interventions

There is an understanding that one intervention alone is insufficient, and psychiatric intervention is not suitable for all cases. The main intervention supported by QFTAC is case management, involving creating a network around the person of interest for social support and monitoring of changes in behaviour (Wilson et al., 2021). The Victoria FTAC collaborates with dedicated drug and mental health counselling services for FTAC cases (Wilson et al., 2021).

For Project Solus, interventions depend on the nature of identified risk (Pathé et al., 2018):

- Mental health need: for those with mental illnesses needing treatment and support, QFTAC liaises with services to facilitate access to resources and provide information to those services. This might include referrals to the Queensland Living Safer Together Intervention Program.
- Law enforcement need: where there is still a law enforcement risk but no mental illness where mental health or behavioural interventions could help.
- Mental health and law enforcement need: mental health input is required but the level of concern can only be reduced by complementing this with counterterrorism investigation, intervention, and monitoring.

Case management structure

There are weekly multidisciplinary case management meetings, and cases remain open until reduced to low concern (Pathé et al., 2018). The Risk Aide-Mémoire is readministered before closing the case, or if there is a change to circumstances.

Quality/standards assurance

Data collection and record keeping practices

QFTAC preserves confidentiality through separate computers and filing systems for the police and mental health staff (Pathé et al., 2018).

Data sharing between agencies

Similar to FTAC, restrictions on sharing health information is a barrier to this multi-agency approach. However, more often, it is police information being shared with psychiatric professionals that is important, so that clinicians are fully aware of the content and context of threatening communications (Wilson et al., 2021). There is also a Memorandum of Understanding dictating data sharing between Queensland Police Service and Queensland Health, which details exceptions to confidentiality requirements, including for public safety (Pathé et al., 2018).

Violent Extremism and Lone Actor Grievance-Fuelled Violence

Community Connect

Summary

Community Connect was a multi-agency community team aiming to put youth at risk of violence in touch with services, primarily religious and cultural, to solve issues manifesting in or causing violence risk, according to the social ecological model of radicalisation. The team incorporated multiple community service leaders to facilitate introductions and referrals to services, and monitor the case until engagement with those services was stable.

Threat assessment set up

Background and objectives

Community Connect was borne out of the social ecological model of radicalisation where, given there is no single pathway or risk factor, no isolated intervention will be effective and a multidisciplinary response is required (Ellis et al., 2022). A meeting of stakeholders and community leaders of different disciplines was arranged to share perspectives on the barriers they noticed in their respective services, which was often noted to be a lack of culturally and religiously appropriate services. Overall, the consensus was that preventing violent radicalisation requires addressing other community, individual, and family issues, both to address common issues and generate trust in services. A particular issue in team formation was incorporating law enforcement yet maintaining trust of other necessary social, mental health and faith-based services. This trust was generated over time through consultation, collaboration, and an agreed prevention approach.

Threat

Violence of any form, primarily violent radicalisation and gang violence. In practice, this also included school violence, self-harm, domestic violence, and sexual aggression.

Basic information:

- Country: United States
- Setting: Community
- Date of formation: Operational from 2017 to 2019
- Remit: Youth up to age 24 at risk of violence or criminal justice system involvement and where needs are not sufficiently met by existing mainstream services.
- Funding: The team rejected the idea of funding from federal law enforcement or intelligence agencies as this would alienate community services. The team supported itself with grant funding, and individual interventions were funded by other means e.g. insurance, grants, and community agency contracts.

Team details

Specialist vs. multidisciplinary

Multidisciplinary: Community Connect was a multidisciplinary and multi-agency team, including leaders from diverse service backgrounds. Involvement of law enforcement was received reluctantly by other members of the team due to trust, criminalisation, and stigmatisation, so trust was built over time and with data-sharing limitations.

Team structure

The full team consulted on cases, but a trusted liaison was assigned for contact with the youth and family, which was generally the agency leader who referred the case to the team. The team met monthly, where meetings began with each team member explaining their agency, resources, ethics, and terminology to others. When interventions were galvanised, a services team consisted of all relevant agencies with one Community Connect member, who served as the services team lead and ensured the team, youth, family, and services were kept informed.

Core team

Community Connect consisted of representatives from:

- Faith based services
- Mental health
- Education
- Community leaders
- Local law enforcement

Referrals structure

Case generation

Member agencies referred to the team anyone involved in their services who they judged to be at risk of violence or criminal justice system involvement. Around a quarter of referrals also came from local FBI field offices, though the FBI was not a formal partner and did not attend meetings or have access to shared information.

Contact with referring bodies

If the referral originated with the FBI, the team informed them if the case was accepted or declined, or service engagement was terminated.

Threat assessment operations

Threat assessment process

The Community Connect process was as follows:

1. Referral made by member agency.
2. Triage for imminent risk: team reviewed for imminent risk of violence, and if so referred to law enforcement or mental health.
3. Case acceptance: where criteria were risk for criminal justice system involvement and needs unmet by existing services. The team could accept, reject, or merely provide consultation on a case.
4. Assignment of trusted liaison: if accepted, a mental health member and 'trusted liaison' (generally the referring member) met the youth and their family to explain Community Connect, gain consent or assent, and sign releases of information.
5. Psychosocial assessment: where goals were understanding the youth and family's concerns, in order to refer them later to services that they will trust and not reject. Collateral information was gathered and the full assessment was brought to the team where different disciplines suggest services and support options.
6. Formation of services team: based on team recommendations and family opinions, an action plan as developed including referral to services. A services team was

formed, of the relevant intervention agencies and a member of Community Connect (the services team lead).

7. Ongoing consultation to services team: the team provided consultation to the services team where necessary, e.g. regarding religious or cultural background, or violent radicalisation. The services team monitored risk level, and ensured good communication with the youth and family.
8. Termination: the team ceased involvement when the youth has been stably engaged with services for around 6 months. The youth and family could withdraw at any time, in which case the team tried to understand and address concerns.

Remote vs. in person threat assessment

In person: the mental health professional and trusted liaison discussed with youth and their family.

Threat assessment output

Main outputs were an action plan including referral to services and creation of a services team.

Interventions

In-house interventions

The main intervention was referral to services, preferably those that already exist in the community, and the services team lead coordinating communication.

Outsourced interventions

Referral services could include mental health, religious mentors, family support services, events in the community, social workers, psychologists, medical advocates. There was a major focus on helping with religious and cultural issues.

Case management structure

The services team lead kept in touch with the youth and family, often with weekly check-ins over text or informal meetings in the community. After 6 months of stable engagement with referred services, the team ceased involvement in the case.

Quality/standards assurance

Data sharing between agencies

Data sharing was a key point of contention given the reluctance to include law enforcement involvement. While law enforcement members were committed to supporting the youth, they would have to act on information if heard, and it was therefore agreed they could be asked to leave team discussions. The team did not provide information to the FBI. Releases of information stated that information would be shared if required with local law enforcement only if there was a risk of violence, who would then contact the FBI if necessary. Other standard confidentiality practices in mental health applied.

FBI Behavioral Analysis Unit-1's Behavioral Threat Assessment Center

Summary
The FBI BAU-1's Behavioral Threat Assessment Center (BTAC) is a key part of the FBI's aims to build the threat assessment and management capacity nationwide. The multidisciplinary BTAC team takes on the most complex cases, and provides training and consultation to FBI field offices.

Threat assessment set up

Background and objectives
The BTAC is the first federal multi-agency and multidisciplinary task force for preventing terrorism and targeted violence through threat assessment (Gibson, 2023). It is key to the FBI's fundamental aim of preventing crimes before they occur, particularly in response to increasing mass casualty events and financial liabilities resulting from missed opportunities before attacks. While this is a challenging objective given the prevalence of juvenile involvement and lack of law-breaking so far, the overarching principle is there are opportunities for disruption and prevention due to the time taken to plan and develop grievances, and observable pre-attack behaviours. The BTAC's main role is to support threat assessment of the most concerning law enforcement cases in the country.

Threat
Terrorism and targeted violence. In practice, the BTAC responds to threats of active shooters, school shootings, workplace violence, and stalking. In 2022, it partnered with the FBI Counterterrorism Division, who can make referrals to the BTAC and receive courses on applying threat assessment to their investigations.

Basic information
- Country: United States
- Setting: Law enforcement
- Date of formation: 2010
- Remit: Nationwide
- Location: Central BTAC and field office teams

Other involvements
The BTAC's wider role is leading the national Threat Assessment and Threat Management initiative, to enhance and train the threat assessment and management capability in the FBI and its field offices. The BTAC also conducts post attack analysis, research on pre-attack behaviours and leakage, and comparisons of active shooters with individuals of concern. They host annual FBI task force training conferences, and mental health practitioners' conferences to educate on threat assessment.

Team details

Specialist vs. multidisciplinary
Multidisciplinary: to leverage partnerships and incorporate members from other teams and government departments who can draw upon diverse resources, including mental health, probation and parole, social services, law enforcement, department of defence, education, religious services, city and state departments, and national resources like the BTAC.

Team structure

There were 19 BTAC members in 2023. As this is an FBI unit, special agents lead investigations. Aside from the core BTAC, each field office has at least one member with advanced BTAC training, who is the point of contact for local threat assessment building. These field offices can have their own threat assessment teams and can request BTAC support.

Core team

BTAC staff include:

- Special agents
- Analysts
- Mental health professionals
- Researchers
- Prosecutors

Additional part time or consulted disciplines

The model is based on having a core team of key disciplines, and an affiliate team who can be engaged when necessary.

Referrals structure

Case generation

Referrals generally originate from local FBI field offices to the BAU-1, and then to BTAC. For terrorism cases, some originate from the Counterterrorism Division, who refer complex investigations to BTAC.

Threat assessment operations

Threat assessment process

There are three key steps in the BTAC threat assessment process:

1. Data-gathering: including context (mental health status, life stressors), mindset (ideology and attitudes), capability, signs of imminence, and protective factors.
2. Threat identification: including specifics of location, methods, and targets.
3. Dynamic formulation: information is organised into risk factors, protective factors, precipitating factors, and perpetuating factors, to inform threat management. This is formed through multidisciplinary discussion.

Risk assessment instruments used

The BTAC uses an SPJ approach for targeted violence and terrorism, including adapted versions or combinations of the Structured Evaluation of Extremist Risk (StEER) and other tools.

Quality/standards assurance

Performance and efficacy evaluations

BTAC researchers compare active shooters with individuals of concern, where none of the latter have become violent or progressed to an attack once referred to the BTAC.

Data sharing between agencies

Data sharing is critical to multi-agency working but limited by privacy acts, meaning the BTAC consults with legal experts.

Channel Programme

Summary

The UK Channel Programme is a multi-agency collaboration to assess and manage individuals with vulnerabilities towards violent extremism.

Threat assessment set up

Background and objectives

The Channel Programme is part of the UK government's Prevent strategy, which aims to stop individuals being radicalised into involvement in violent extremism. Channel involves multi-agency assessment and management, based primarily on the Vulnerability Assessment Framework (VAF) instrument alongside other guidance documents (Gill & Marchment, 2020). The VAF uses risk factors from the ERG22+ and, before that, the SRG. Both were used in offender management contexts, whereas the VAF can be applied to any individual referred to Prevent. Its objective is to aid decision-making regarding whether and how to intervene with individuals on a path towards radicalisation.

Threat

The targeted threat is violent extremism. VAF guidance states that it can be used on all forms of extremism, but its foundations and research bases are in Islamist extremism.

Basic information

- Country: United Kingdom

Team details

Specialist vs. multidisciplinary

Channel is a multi-agency programme, but the VAF is usually filled out by counterterrorism police.

Team structure

Those involved in Channel include but are not limited to counterterrorism police, Prevent officers, Channel panel coordinators, interventions providers (IPs), VAF trainers, and policymakers.

Training

Police practitioners that use the VAF should have a good understanding of it. VAF training often involves a substantial session during in person Home Office-led Prevent foundation courses, Hydra training, on the job experience, and ERG22+ training. Gill & Marchment's (2020) report evaluates VAF training through surveys and interviews with practitioners and found a general feeling of a lack of sufficient training, which results in inconsistent and incorrect application of VAF guidance. Around half their participants had training or some form of support in how to use the VAF, in the form of documents, advice from panel chairs, or discussions with colleagues and supervisors. Less than half of participants agreed that training was useful.

Referrals structure

Case generation
Cases are generated by referral.

Threat assessment operations

Threat assessment process
The threat assessment process involves:

1. Referral: referrals are corroborated to ensure they were not made in ignorance or with malicious intentions, and are checked against ongoing police investigations.
2. Information-gathering by counterterrorism police: over a maximum of five working days.
3. Triage: using the Prevent Gateway Assessment Dynamic Investigative Framework (PGA-DIF) to decide if the case should progress to Channel. If so, information gathered up to this point feeds into the VAF later on.
4. Multi-agency information-gathering: when there is urgent action required or a difficulty obtaining corroborating information, this may involve meeting with the individual or their family or friends before the Channel panel and asking questions led by the VAF.
5. Initial VAF assessment and write-up: this can take several hours and should be completed by a counterterrorism police practitioner with a solid understanding of the VAF, with advice from a team or supervisor and led by the VAF guidance document.
6. Risk assessment.
7. Section 36 decision: by a counterterrorism police supervisor, regarding whether to progress the case to the Prevent Multi-Agency Panel (PMAP) process.
8. Case adoption or rejection by the Channel panel: panel chairs and partners are given the VAF to review before the panel.
9. Consent: a suitable agency ensures there is consent from the individual to receive Channel support.
10. Channel panel: the VAF is presented, and from now on is a dynamic assessment instrument. It is updated at least quarterly, sometimes after each intervention or when new information is received, including through contributions from other agency partners. The panel chair decides whether to proceed, led by the VAF. If so, the panel suggest risk management strategies. While the VAF does not dictate case management plans, it can help identify intervention options based on risk and protective factors.
11. Interventions: often involving updates to the VAF.
12. Intervention completion and case closure.
13. Case review: the case is reviewed at 6 and 12 months. If the case is adopted, it must be reviewed when closed.

At any point in this process, the case might be rejected because it is closed, referred to other services, escalated to police, or has had consent withdrawn.

Resources used in threat assessment
At the first point of referral there is limited information. To get a more accurate assessment, the VAF is updated as more information comes in from more sources, including interventions providers.

Risk assessment instruments used

The VAF is the instrument used within Channel. The VAF is continually updated for each case at least quarterly, particularly with information from in person interventions, as there is limited information known when initially filled out. Assessors rate the level of evidence for risk factors in three domains: engagement, intent, and capability. Unlike its predecessors, the VAF is purely for assessment and does not include any guidance on risk management. It also does not include scenario planning or case formulation of individual risk judgements and explanations. In this sense it is seen as an SPJ-lite tool. Some Channel units supplement the VAF with their own risk formulation templates, or with the ADASS Guidance Safeguarding Risk Assessment Tool, Asset+, RADO, SPLICE, and others.

The PGA-DIF is the triage tool used to decide to progress the case to Channel. This is a simple tool and less subjective than the VAF, though with a different objective. The main differences are that it is more focused on protective factors, covers more ideologies, and involves an action plan.

Remote vs. in person threat assessment

The Channel process does involve engagement with the individual referred, but usually not before the initial VAF write-up. When there is urgent action required or a difficulty obtaining corroborating information, this may involve meeting with the individual or their family or friends before the Channel panel and asking questions led by the VAF. The VAF is continually updated, for example with input from interventions providers who have in person interactions with referred individuals. They correct information and can identify protective factors, which are all fed back into the VAF.

Threat assessment output

The main output of the threat assessment process is the completed VAF, and an intervention and management plan.

Interventions

As a multi-agency collaboration, interventions can be outsourced to many agencies, including interventions providers or for heath assessments. Interventions providers are often assigned with specific tasks guided by the VAF's risk and protective factors. They often request a copy of the VAF to have as much information as possible, and provide feedback and reports that are used to update the VAF.

Case management structure

Cases are reviewed at 6 months and 12 months, and upon closure.

Quality/standards assurance

Performance and efficacy evaluations

Gill & Marchment's (2020) report evaluates user perceptions of the effectiveness of the VAF. They found that just over half of participants agreed the VAF is useful, gives confidence in decision making, and helps with structuring.

Data collection and record keeping practices

The VAF is often shared with Channel panel chairs and partners before the panel, through there are often concerns about security and unnecessary volumes of material being shared. VAF documents are kept and updated, including with feedback and reports from interventions providers, some of whom complete their own VAF documents.

Dutch National Police investigative psychologists

Summary
Dutch National Police (DNP) specialist investigative psychologists, along with other disciplines, consult on potential violent extremism cases with police and do not themselves interview subjects. They use multiple risk assessment instruments and triage processes to deliver recommendations to the DNP on risk management, more information-gathering, or strategies to communicate with the subject.

Threat assessment set up

Background and objectives
Due to the disproportionate prevalence of psychosocial issues and psychopathology among potentially violent extremists, the DNP involve investigative psychologists in these cases (Bootsma & Harbers, 2021). Each of the DNP's 11 units have at least two investigative psychologists. Investigative psychologists perform assessments to aid operational decisions into monitoring, protective security, and investigative strategy. Their focus is on the individual subject of concern, and their life course and specific risk and protective factors, both static and dynamic.

Threat
The targeted threat group are potential violent extremists, from multiple ideologies: jihadist, left ring, right wing, and single issue.

Basic information
- Country: Netherlands
- Setting: Law enforcement
- Date of formation: The model began in the late 2010s and remains a work in progress.

Team details

Specialist vs. multidisciplinary:
Multidisciplinary: the full-time team is specialist, but external experts are consulted for assessment and advice, and the overall approach to a case involves a combination of policework and consultation from investigative psychologists.

Team structure
Ideally, at least two investigative psychologists work together on a case, reading all the information and judging the presence of risk indicators, coming together at the end to make a collaborative decision.

Core team
The core full-time team contains only investigative psychologists within the police.

Additional part time or consulted disciplines
Other agencies and disciplines can be involved through various mechanisms. When referrals come from outside the police, there is a multiple agency case meeting to share information, perspectives, and concerns. This can include prosecutors, police, parole, mental health services, counter terrorism, intelligence, healthcare, housing services, and debt services. It

often takes the form of a 'Local Safety Center'. Also, it is recognised that investigative psychologists are not specialists in terrorism, so it is recommended that they consult with other experts from counterterrorism, psychiatry, social psychology, intelligence units, and subject matter experts in countries or weapons. In particular, intelligence departments aid the process by identifying subjects of concern, gathering information, and assessing the level of radicalisation or attack planning. These experts are encouraged to give their perspective, listen to others, and remain within their specialism, to come to a multidisciplinary perspective and range of mitigation plans that takes all perspectives into account and prevents any bias or groupthink. Meetings with experts are led by the investigative psychologists working on the case.

Training

Investigative psychologists working on these cases have academic backgrounds with an expertise in risk assessment of violence, though do not have an expertise in terrorism so consulting outside experts is needed. They keep up with scientific developments in their research field.

Referrals structure

Case generation

Cases are referred to the investigative psychologists by the DNP, though the initial referral to the DNP may come from external agencies.

Threat assessment operations

Threat assessment process

Investigative psychologist involvement develops as follows:

1) Referral from DNP.
2) Intake and triage: the investigative psychologists do not consult on all cases. Cases must meet certain criteria relating to suspected presence of a mental health problem and concern for future violence. At triage, the team clarify their role in involvement in the case, the cause for concern, the question being asked, the information gathered so far, and the urgency. They use triage questions related to the pathway to intended violence. They also here choose a working method, usually a situational professional judgement (SPJ) framework.
3) Information-gathering: to assess risk.
4) Construction of a behavioural timeline: this is a life-long timeline of observable behaviours and known facts, not judgements. These include life events, behavioural development, personality traits, social networks, actions and reactions, warning behaviours, threatening communications, and their precise wording. Understanding that people are shaped by their experiences more than their personality, the team are looking for indicators of changes, escalation, or de-escalation.
5) Consultation with external experts: any outside experts that are being consulted upon will read the behavioural timeline and engage in a meeting, chaired by the investigative psychologists.
6) Risk assessment.
7) Risk formulation: a causal explanation and theory of the concerning behaviour. They employ visualisations and mind maps to understand the multiplicity of motivating factors.

8) Scenario planning: determining potential scenarios and their imminence and likelihood. Scenarios are focused on violent attack in the Netherlands and violence facilitation through other actions including recruiting or becoming a foreign fighter.
9) Recommendations to DNP.

Resources used in threat assessment

The volume of information gathered depends on many factors including the time the subject of concern has been known to the police, and the fact that the team have limited time to provide their findings meaning they cannot always do a full written report. Police provide access to confidential information including reports, comments from the subject to police, secret recordings from communications, court orders, expert opinions, parole officer reports, and behaviour in custody. Open-source information includes social media and internet history, when the subject's phone or computer has been seized. Other information sources can include political activity, criminal records, and observed changes in daily routines.

Risk assessment instruments used

During risk assessment, the team uses an SPJ approach. The DNP team have developed a work-in-progress best practice procedure based on the SPJ approach to ensure it is flexible and person-centred. As the SPJ approach dictates, for a systematic approach they use a toolbox of risk assessment instruments together, dependent on the case. The toolbox includes HCR-20 version 3, MLG, TRAP-18, VERA-2R, and IR-46 by collaborating with intelligence units to assess level of radicalisation. Risk factors from these instruments are treated more as risk indicators, and the team use professional judgement to determine their relevance to the case. They use the behavioural timeline to look at the relevance of risk indicators in relation to each other, focus on those especially relevant to violent extremism, proximal warning behaviours, and indicators that are supported by recent literature distinguishing between attackers and non-attackers.

Remote vs. in person threat assessment

The investigative psychologists investigate from afar using observable behaviours and diagnoses from other sources. They do not perform clinical interviews on the subject or otherwise interact with them. They do, however, conduct interviews with police colleagues to understand more about information gathered before their involvement.

Threat assessment output

The main output is recommendations for the DNP. Others include the behavioural timeline and risk formulation.

Interventions

In-house interventions

The investigative psychologists do not perform any in-house interventions.

Outsourced interventions

They give recommendations to the police, in three forms. Firstly, they may give input into risk management, using the risk formulation and management strategies provided by tools such as HCR-20 v3. They might recommend a forensic evaluation by a psychologist or psychiatrist for involuntary treatment. Secondly, they might recommend more information-gathering as

a part of the monitoring strategy. Finally, they might recommend ways to approach, communicate, and establish rapport with the subject of concern.

Case management structure

Monitoring is a primary recommendation that might be made to police.

Quality/standards assurance

Performance and efficacy evaluations

The investigative psychologists keep up with evolving science and empirical findings in their area, given the lack of established SPJ tool or evidence base for risk factors for violent extremism.

Mixed Threat Forms and Problem Behaviours (e.g., general violence, stalking, threats)

FBI Behavioral Analysis Unit model for analysing anonymous threatening communications

Summary
The FBI Behavioral Analysis Unit (BAU) assesses anonymously communicated threats referred by law enforcement agencies. Through the assessment process, there is significant emphasis on procedures to prevent bias and groupthink. The BAU does not carry out interventions but recommends monitoring and intervention strategies back to the referrer.

Threat assessment set up

Background and objectives
Most threatening communications received by the FBI BAU are anonymously authored and sent, and this is increasing partly due to the internet (Simons & Tunkel, 2013; 2021). The BAU takes all threats seriously, but when they are anonymous, threat assessment cannot include any information on the offender and their personal or criminal history. The BAU therefore has a specified process for these anonymous threatening communications.

Threat
Anonymous threatening communications.

Basic information
- Country: United States
- Setting: Law enforcement

Team details

Specialist vs. multidisciplinary
The procedure involves a specialist team. However, there is an emphasis on all team members discussing and peer reviewing the final product, while embracing debate to avoid groupthink or individual bias, and to combine perspectives from different disciplines and training (Simons & Tunkel, 2021).

Team structure
All cases are looked at by a team, rather than an individual (Simons & Tunkel, 2013). A team leader collects information, selects other team members, organises assessments and consultations, and writes written assessments for referrers (Simons & Tunkel, 2021). To avoid confirmation bias, the team includes a 'lone assessor' who is separated from all investigative findings, suspect information, and context and only presented with the anonymous communication. They return to the group and present their view before gaining any contextual information.

Additional part time or consulted disciplines
Cases can be looked at by core team members or ad hoc specialists (Simons & Tunkel, 2021).

Training
All team members should have training in threat assessment (Simons & Tunkel, 2013).

Referrals structure

Case generation

Referrals are made by federal, state, or local law enforcement agencies who request BAU assistance (Simons & Tunkel, 2021). The threats they refer take many forms, including verbal, written, hoax, cyber extortion, and threat waves.

Threat assessment operations

Threat assessment process

The process is as follows:

1. Referral received and team leader designated: the lead checks that no other threat assessment individual or team is currently analysing the same communication (Simons & Tunkel, 2013; 2021).
2. Triage: the leader collects limited available information on the content and background of the communication, including how the threat was delivered, frequency and intensity of threats, feasibility of threatened attack, potential targets, and level and method of anonymity (Simons & Tunkel, 2021).
3. Individual threat assessment: each team member receives this information, except the lone assessor who only receives the communication (Simons & Tunkel, 2013; 2021). All individually complete an assessment through looking at: mode of delivery, victimology and relationship with the target, linguistic staging, motive, level of veracity, resolution to violence, and imminence of the threat.
4. Group threat assessment: the lone assessor joins the group and delivers their assessment. All members re-assess, check for bias, and reach a final collective opinion on the level of concern, not level of risk (Simons & Tunkel, 2013; 2021).
    a. Low concern: might require more information or monitoring.
    b. Moderate concern: possible violence, but not urgent. Requires monitoring and further information or action.
    c. Elevated concern: reaching a critical point on the pathway to violence, so requiring time imperative action for the target.
    d. High concern: violence possible in the future if there is a catalyst event.
5. Telephone consultation: the assessment is summarised to the referrer over a phone or video call with opportunity for questions (Simons & Tunkel, 2013; 2021). This includes risk factors, protective factors, potential catalyst events, and their overall assessment.
6. Written report: the assessment is written, peer reviewed, and delivered to the referrer (Simons & Tunkel, 2013; 2021)

Resources used in threat assessment

Due to the communications being anonymous, resources are limited to the content of the threat and other information surrounding it (e.g., mode of delivery).

Remote vs. in person threat assessment

As the threats are anonymously written, all threat assessment is remote.

Threat assessment output
The final output is a peer reviewed written assessment and telephone consultation with the referrer, involving a collectively decided judgement on the level of concern and imminence of violence (Simons & Tunkel, 2013).

Interventions

In-house interventions
The BAU does not carry out any interventions.

Outsourced interventions
In the telephone consultation the BAU team provides threat management recommendations to for identifying the author, protecting the victim, mitigating violence, and interviewing (Simons & Tunkel, 2021).

Quality/standards assurance

Data collection and record keeping practices
Final written assessments are recorded (Simons & Tunkel, 2021). The BAU has a Communicated Threat Assessment Database to record threats, which was merged with the FBI's Anonymous Letter File in 2012 (Simons & Tunkel, 2013). This allows assessors to identify patterns in content and delivery of threats, and record outcome data.

San Diego Stalking Strike Force's Stalking Case Assessment Team

Summary
The San Diego Stalking Strike Force's Stalking Case Assessment Team (SCAT) is a voluntary, multidisciplinary team that analyses and manages stalking threats with a key focus on victim education and safety planning.

Threat assessment set up

Background and objectives
The SCAT was formed partially in response to the murder of an attorney in 1989, which highlighted stalking as pre-attack behaviour and intervention opportunity (Maxey, 2002). At the time, there was no threat assessment team to call upon nor any stalking legislation. The SCAT was created through surveying counsellors, social workers, and therapists for the nature and scope of stalking, and through determining a severe under-reporting and lack of management from police records. It is borne out of the premise that multidisciplinary approaches are most effective, and it serves as a model for using this to address complex problems through assessment, monitoring, and re-evaluation.

Threat
Stalking.

Basic information:
- Country: United States
- Date of formation: Stalking Strike Force formed in 1994, SCAT set up in 1996.
- Remit: San Diego County
- Funding: involvement in the team is voluntary, and there are no federal grants or departmental budgets.

Other involvements:
The team trains law enforcement, prosecutors, and mental health professionals. It also holds conferences to train on stalking, bring disciplines together, feature victims and survivors, and share information and resources. They have also created educational videos on stalking, workplace violence, and threat assessment, and lectured to schools, community organisations, and law enforcement both in the US and abroad. The team also has a victim support and education role, with a committee of advocates and survivors having published a handbook of information, guidelines, safety tips, and support groups.

Team details

Specialist vs. multidisciplinary
Multidisciplinary: all disciplines agreed more needed to be done to combat stalking, and they should bring together their resources and knowledge.

Team structure:
The SCAT meets monthly and on call.

Core team
The SCAT comprises:

- Local, state, and federal law enforcement officers
- Prosecutors
- Mental health professionals: forensic psychologists who provide unique expertise, dynamic assessments, and management strategies.
- Victim advocates

Additional part time or consulted disciplines
The SCAT can also incorporate probation officers for insight into management for the post-conviction and release phase.

Threat assessment operations

Resources used in threat assessment
Family court files have proven invaluable to the team, as they are publicly accessible and provide information on weapons and domestic violence history.

Interventions

Outsourced interventions
The main intervention is providing management strategies, particularly considering not all cases reach prosecution. These include victim education, safety planning (restraining orders, physical security, counselling, change of identity), surveillance, and investigation.

Case management structure

As stalking is dynamic and cases are long term, assessments are frequent to update and review communications and their mental health status. The team continues throughout to provide victim safety advice and support, and liaise with the state parole office for post-release management.

Willamette Valley Adult Threat Advisory Team

Summary

The Willamette Valley Adult Threat Advisory Team tackles a wide range of threats and aggressive acts in by bringing together a large multi-agency community team. Each agency can refer, advise on, and recommend interventions for each case.

Threat assessment set up

Background and objectives

The team began as a partnership between law enforcement, the Salem-Keizer school district, and state courts (Van Dreal & Okada, 2021). It was born out of the recognition that one team cannot always handle both youth and adult cases due to the differences in risk factors, resources, and legal, educational, and ethical complications. There may still be overlap in membership between youth and adult teams, and overlaps in cases, for example in cases of domestic violence related to a school.

Threat

This team looks at threats or acts of aggression, in areas including domestic violence, workplace violence, stalking, and threats to public officials, courts and schools. This is not restricted to targeted violence, and could be concerns to the whole community.

Basic information

- Country: United States
- Setting: Community
- Date of formation: The Marion County Adult Threat Assessment Team was formed in 1998, prompted by a series of high-profile targeted attacks in Salem, Oregon in the 1990s. This later became known as the Willamette Valley Threat Advisory Team.

Team details

Specialist vs. multidisciplinary

Multidisciplinary. This is a community based and multi-agency collaboration that shares resources, experiences, and training to identify and mitigate situations where there is potential for violence. All team members have the support of their respective agency and must be comfortable providing their perspective and input, even when it conflicts with others.

Team structure

Each member agency chooses a representative based on their experience, perspective, and expertise, ensuring that all team members have the support of their respective agency to make quick decisions and actions. The lead on a particular case is the representative from whichever agency from which the case arose. They present the case to the team and assume the role of case manager.

Core team

The core team usually includes representatives from several community agencies, including public mental health services, law enforcement, educational institutions (including higher

education), district attorney offices, domestic violence response teams, parole and probation services, court security, and other government agencies.

Referrals structure

Case generation

Cases are generated through referrals concerning the perception of a threat. This could be inappropriate communications, pre-attack behaviours, or other suspicious activities. Referrals come in to one member agency, who triage this threat and present to the multi-agency team.

Threat assessment operations

Threat assessment process

1. Triage: before the team meeting, the agency that received the referral triages the case to determine if it gets passed to the multidisciplinary team, using a protocol for assessing targeted violence in adult populations. This is similar to a level 1 assessment in the Salem-Keizer/Cascade school violence model.
2. Presentation of case: this case manager agency representative presents to the multi-agency team. They may also have asked before this for help from other team members to gather more information.
3. Assessment: the team carries out further assessment if needed and advises on risk factors, behaviours of concern, investigative strategies, and recommended management plans, both short term and long term.
4. Implementation and intervention: this remains with the case managing agency.

Threat assessment output

Outputs from assessment by the larger team are recommended investigative strategies and management plans.

Interventions

Interventions are drawn from the case managing agency and their network of other community resources.

Quality/standards assurance

Data collection and record keeping practices

To aid integrity and ownership of information, each member agency is responsible for its own materials, resources, notes, and records. The team does not keep records beyond this.

Data sharing between agencies

All member agencies are aware of their agency's rules on confidentiality and sharing information outside that agency, with public safety always being prioritised.

Forensic Assessment and Case Management Unit within the Cantonal Threat Assessment and Management model

Summary
The Forensic Assessment and Case Management Unit (FACMU) is a joint police and mental health unit of experts within the Cantonal Threat Assessment and Management (CTAM) model in the Canton of Zurich to protect public figures and private citizens from problem behaviours. FACMU forensic experts provide consultation to threat assessment and management (TAM) police units, creating an interdisciplinary approach.

Threat assessment set up

Background and objectives
The FACMU was part of the CTAM approach, and one of its main purposes is to support police TAM units (Guldimann et al., 2016). This was inspired by many other threat assessment and management units looking to identify, assess, and manage the risk to public officials that incorporate mental health units. The FACMU aims to prevent, rather than predict, violence, using long term violence assessment, rather than short term risk assessment. This was a change for forensic professionals who usually were called in by prosecution after an offence was already committed. The FACMU was initially named the Forensic Assessment Unit (FAU), but this was changed to reflect the emphasis on case management to supplement assessment.

Threat
Problem behaviours (domestic violence, stalking, and others) directed at public or private individuals, with an understanding that violence is dynamic and one incident can transform into new targets, motivations, or types of violence over time.

Basic information
- Country: Switzerland
- Setting: Law enforcement
- Date of formation: The FAU was started in pilot form as a part of the CTAM approach in 2014. In 2015 it was made a full unit and changed its name to the FACMU.
- Remit: Canton of Zurich
- Funding source. The Department of Health, Department of Justice and Home Affairs, and Department of Security jointly funded a two-year pilot. Forensic practitioners were employed by a university.
- Team location: Department of Prevention, in Cantonal Police of Zurich. FACMU forensic professionals and TAM police share offices on the same floor to facilitate communication and collaboration.

Other involvements
The FACMU supports public prosecutors in need of a quick decision for pre-trial custody or prison release. This is in the form of short-term assessments based on casefiles and interviews, not a full risk assessment that a forensic expert would normally provide a court. The aim is to help decide an action plan and reduce the likelihood of a wrong decision on incarceration. The FACMU also provides supervision to general psychiatric clinics assessing and managing risk of violence, and membership of Interdisciplinary Expert Panels in urgent and complicated police cases.

Team details

Specialist vs. multidisciplinary

Interdisciplinary: the FACMU's guiding principle is collaborating by gaining and sharing information and perspectives from many sources. This is emphasised by the joint funding by 3 different stakeholders. The presence of mental health practitioners in interviews helps in situations where the person of interest has a previous grievance towards the police (or vice versa), and aids communication between police and the psychiatric team for the person of interest.

Team structure

The FACMU support police TAM units, and are never the lead on a case. They join case discussions, join interviews with persons of interest, write up forensic assessment reports, explain psychiatric terms, help in communication between police and psychiatric services, provide non-mandatory recommendations, and ensure adherence to professional standards regarding psychiatric assessment, risk assessment, and interventions.

Core team

The core team working on threat assessment cases include:

- Police within the TAM units
- Forensic experts in the FACMU: these help police through understanding of psychiatric disorders, how these relate to criminal behaviour, and risk assessment instruments. They support the process by interviewing persons of interest, assessing risk for violence, providing counselling, and providing management strategies. Forensic practitioners are familiar with predicting violence, so must adjust away from this towards a prevention perspective.

Referrals structure

Case generation

There is a dedicated 'contact person' in all municipalities, child and adult protective services, domestic violence counselling services, and other public authorities in the Canton of Zurich. This person is the liaison between the workplace and the Service for Protection against Violence (SPV) to enable referrals to the SPV and then the FACMU. Contact persons receive training workshops on the CTAM approach, and checklists regarding concerning behaviours to help them decide if they need to escalate the case to SPV for evaluation. Contact persons are the only ones to see information on problematic cases of behaviour and communications.

Contact with referring bodies

Beyond training contact persons, there is also training for public officials, including the police. This includes training on victimisation, stigmatisation and negative attitudes arising from being stalked, in an effort to encourage reporting.

Threat assessment operations

Threat assessment process

The FACMU process follows:

1. Triage: while there are no exclusion criteria for the FACMU, certain factors must be present, to keep the caseload at a manageable level. There must be suspected risk-related psychopathology, warning behaviours, change in behaviour or loss of support system, and fear or intuition of the victim, referrer, or professional involved in the case.
2. Interview: forensic experts join police on interviews with persons of interest.
3. Report: they summarise risk potential, scenario planning, and management plans in a forensic assessment report.

Risk assessment instruments used
Actuarial instruments (e.g., ODARA) are used to compare to other offenders. SPJ instruments (e.g., SAM) are used for static and dynamic risk factors, and to help with scenario planning.

Remote vs. in person threat assessment
Police and forensic experts from the FACMU conduct interviews with the person of interest.

Threat assessment output
The main output is the forensic assessment report, summarising findings regarding risk, scenario planning and recommended interventions.

Interventions

In-house interventions
There are no in-house interventions by the FACMU, but TAM police can carry out some interventions, including issuing contact orders and denying requests for gun licenses.

Outsourced interventions
Interventions usually involve recommending medication, recommending strategies to the police, and creating networks around the person of interest to monitor them. At the time of publication, a forensic outpatient facility was in creation where subjects can be transferred based on either consent or a disciplinary measure, as done already in Germany.

Quality/standards assurance

Performance and efficacy evaluations
The FACMU is part of an Interdisciplinary Expert Commission that aims to improve the CTAM approach by identifying problems and solutions.

Data sharing between agencies
Data protection restricts access by the FACMU to police, justice, or mental health systems, and vice versa. With consent from the person of interest, or within legal guidelines concerning information sharing to prevent violence, institutions can be provided with the FACMU's
forensic assessment report.

Problem Behavior Program

Summary
The Problem Behavior Program (PBP) is a specialist clinic of forensic psychologists and psychiatrists. The main role of the PBP is to provide assessment and treatment recommendations, but in high priority cases where needs are not met by other services, they also provide treatment in-house. The PBP targets a range of threats and its main focus is on referring, assessing, and treating individuals based on their behaviour, rather than their mental illness.

Threat assessment set up

Background and objectives
The PBP started when Forensicare, a forensic mental health service, noticed a lack of service provision for high-risk individuals or offenders whose assessment and treatment needs were not being met by existing services, often due to having not yet committed an offence or not having a mental illness (MacKenzie & James, 2011; McEwan & Darjee, 2021; McEwan et al., 2013). There was a realisation that there is a role for forensic clinicians in criminal or problem behaviours driven not necessarily by mental illness but by psychological or social problems (Warren et al., 2005). In the PBP, any referral, assessment, and treatment is based on behaviour, rather than mental illness (MacKenzie & James, 2011; McEwan & Darjee, 2021). It acts as a referral point for criminal justice and mental health agencies, to target problem behaviours and facilitate forensic mental health treatment before they become serious offences (McEwan & Darjee, 2021; McEwan et al., 2013).

Threat
Problem behaviours that lead to physical or psychological damage but do not necessarily reach courts and do not necessarily have a presence of mental illness (MacKenzie & James, 2011; McEwan& Darjee, 2021; McEwan et al., 2013). These can include violence, sexual offences, fire setting, threatening, and stalking (MacKenzie & James, 2011; McEwan & Darjee, 2021; Warren et al., 2005).

Basic information
- Country: Australia
- Setting: Community forensic mental health service
- Date of formation: The PBP was formed in 2003-4, through amalgamating other clinics for certain problem behaviours with or without mental illness presence, including stalking, threatening, and sex offences (MacKenzie & James, 2011; McEwan & Darjee, 2021)
- Remit: Statewide
- Funding source: The PBP was initially funded by Forensicare, a statewide forensic mental health service (McEwan & Darjee, 2021). Due to the adopted approach of not requiring a mental illness diagnosis to justify treatment provision, it has struggled to maintain funding. In 2016, it received further funding from health and justice department funds.
- Team location: Victorian Institute of Forensic Mental Health (Forensicare) in metropolitan Melbourne.

Other involvements

The PBP produces extensive research, through collaborations with Monash University and the Centre for Forensic Behavioural Science (MacKenzie & James, 2011; McEwan et al., 2013). Its clinicians provide education to other organisations, publish in journals, and present at conferences, as well as providing expert opinions in court or to other organisations (Warren et al., 2005).

Team details

Specialist vs. multidisciplinary

The PBP is a specialist forensic mental health unit of psychologists and psychiatrists.

Team structure

The team has weekly intake meetings (McEwan et al., 2013) and all staff can carry out primary and secondary consultations (McEwan & Darjee, 2021). Initial case consultation is done by one or two psychologists and psychiatrists depending on the case, availability, and specialties (McEwan & Darjee, 2021).

Core team

The core team comprises specialist mental health clinicians (McEwan & Darjee, 2021). Most recently, there were 20 psychologists including managers and a neuropsychologist.

Additional part time or consulted disciplines

The team also receives input from psychiatrists, psychiatric registrars, postgraduate internships, and social workers (McEwan & Darjee, 2021; McEwan et al., 2013).

Training

Team members are primarily clinical psychologists with experience and expertise in forensic assessments and interventions regarding offending risk (McEwan & Darjee, 2021; McEwan et al., 2013).

Referrals structure

Case generation

The PBP receives self-referrals and referrals from agencies including courts, correctional services, mental health agencies, private clinicians, and child protective services (MacKenzie & James, 2011; McEwan & Darjee, 2021; McEwan et al., 2013). There is a centralised system where referrals are received by an intake worker who does not have expertise but conducts a structured phone interview to determine how quickly a PBP clinician must be given the case (McEwan et al., 2013; McEwan & Darjee, 2021). They then present to the team at weekly intake meetings.

Contact with referring bodies

Increasingly the PBP provides support to referring agencies while awaiting assessment and recommendations for actions they can take in the meantime or to mitigate the need for referrals (McEwan et al., 2013).

Threat assessment operations

Threat assessment process

The assessment process involves:

1. Referral by another agency.
2. Triage by intake worker: involving structured phone interview (McEwan & Darjee, 2021).
3. Initial consultation and intake meeting: the PBP gives any possible immediate assistance to the referring agency and clarifies details and existing treatment (McEwan & Darjee, 2021). At the intake meeting, the team discuss the level of priority, based on access to weapons, violence history, access to victim, and treatment by other services (McEwan et al., 2013). The case could be kept with the PBP for further assessment or consultation, could be referred to another service, or given back to the referrer with advice to contact again if necessary (McEwan & Darjee, 2021). All cases are allocated to clinicians within two weeks, but high priority cases are within three days (McEwan & Darjee, 2021).
4. Assessment: the subject is allocated to a psychologist or psychiatrist, or both if complex, for an assessment that can take several hours (McEwan et al., 2013). This is supported by psychological tests and structured risk assessment. The aim is to understand motivations behind the problem behaviour and any ongoing mental health issues or psychopathology relevant to it (McEwan & Darjee, 2021; Warren et al., 2005). This culminates in a formulation to explain the behaviour, including risk and protective factors (McEwan & Darjee, 2021).
5. Written report: assessment culminates in a written report for the referrer. The report is authored by both psychologists or psychiatrists, and includes assessment results, psychopathology, motivations, and suggestions for management and treatment, potentially by the PBP (McEwan et al., 2013; Warren et al., 2005).
6. Potential treatment.

Resources used in threat assessment

Clinicians seek information to corroborate interviews, including criminal history, police charge sheets, medical history, previous mental health assessments, and insights from family, friends, police informants, and correctional officers (McEwan & Darjee, 2021; McEwan et al., 2013; Warren et al., 2005).

Risk assessment instruments used

Structured professional judgement tools are used for structured risk assessment. Most often these are HCR-20, SRP, or RSVP (McEwan & Darjee, 2021; McEwan et al., 2013). Tailored psychological tests are also used to assess anger and personality disorders (McEwan % Darjee, 2021). These can include the MMPI (second edition), Wechsler Abbreviated Scale of Intelligence, State-Trait Anger Scale (second edition), and Interpersonal Reactivity Index, among others (Warren et al., 2005).

Remote vs. in person threat assessment

In person assessment of the subject is a central part of the PBP. It takes the form of a two to six hour semi-structured interview to investigate their childhood, employment, relationships, and motivations (McEwan & Darjee, 2021; Warren et al., 2005). The PBP does not contact the victim of the problem behaviour but informs the referring agency of available support services (Warren et al., 2005).

Threat assessment output

The primary output is the written report to the referrer, which includes assessment results, formulation of the behaviour, and risk judgements about persistence and harm for certain behaviours (McEwan & Darjee, 2021; McEwan et al., 2013).

Interventions

In-house interventions

One quarter to one third of referrals receive in-house treatment from PBP psychologists and psychiatrists (McEwan & Darjee, 2021). This depends on level of risk, treatment needs not being met by other services, and the subject's capacity to engage with and benefit from treatment (MacKenzie & James, 2011; McEwan & Darjee, 2021). PBP clinicians can also manage pharmacological treatment (McEwan & Darjee, 2021). They can also provide ongoing consultation when treatment is provided elsewhere (McEwan & Darjee, 2021).

Outsourced interventions

Mostly, the PBP recommends treatment strategies to other agencies, including concerning medications, therapy, offender treatment programs, social skills, emotional regulation groups, informing the target, seizing weapons, or restricting access to certain people (McEwan & Darjee, 2021; McEwan et al., 2013; Warren et al., 2005).

Case management structure

Due to the PBP providing treatment, there are regular reviews to monitor changing risk and progress regarding treatment goals (MacKenzie & James, 2011). Cases are reviewed at the start of treatment, at minimum of six-monthly intervals, and before discharge (McEwan & Darjee, 2021; McEwan et al., 2013)

Quality/standards assurance

Performance and efficacy evaluations

Several studies have evaluated client outcomes and stakeholder perspectives, as well as characteristics of threats (McEwan & Darjee, 2021; Warren et al., 2005).

Data sharing between agencies

While PBP clinicians focus on the patient's best interests, there are limits to confidentiality when there is risk of harm to the patient or others, though agencies often disagree over whether this exception is met (McEwan & Darjee, 2021). Confidentiality limits are explained throughout the assessment and treatment process (Warren et al., 2005).

References

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. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255631406

Barry-Walsh, J., James, D. V., & Mullen, P. E. (2020). Fixated Threat Assessment Centers: preventing harm and facilitating care in public figure threat cases and those thought to be at risk of lone-actor grievance-fueled violence. *CNS Spectrums*, *25*, 630-637. https://doi.org/10.1017/S1092852920000152

Bixler, B. S., Dunn, J., & Grundland, T. (2021). Operations of the Los Angeles Police Department Threat Management Unit and Crisis Support Response Section. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 454-470). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0026

Bootsma, L., & Harbers, E. (2021). Assessing Potentially Violent Extremists: Experiences From Dutch Investigative Psychologists. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 639-653). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0035

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence. *Behavioral Sciences and the Law*, *17*, 323-337. https://doi.org/10.1002/(sici)1099-0798(199907/09)17:3<323::aid-bsl349>3.0.co;2-g

Coggins, M. H., & Pynchon, M. R. (1998). Mental Health Consultation to Law Enforcement: Secret Service Development of a Mental Health Liaison Program. *Behavioral Sciences and the Law*, *16*, 407-422. https://doi.org/10.1002/(SICI)1099-0798(199823)16:4<407::AID-BSL318>3.0.CO;2-W

Cornell, D. G. (2003). Guidelines for responding to student threats of violence. *Journal of Educational Administration*, *41*(6), 705-719. https://doi.org/10.1108/09578230310504670

Cornell, D. G. (2013). The Virginia Student Threat Assessment Guidelines: An Empirically Supported Violence Prevention Strategy. In N. Böckler, T. Seeger, P. Sitzer, & W. Heitmeyer (Eds.), *School Shootings: International Research, Case Studies, and Concepts for Prevention*. Springer. https://link.springer.com/book/10.1007/978-1-4614-5526-4

Cornell, D. G. (2018). Threat Assessment. In H. Shapiro (Ed.), *The Wiley Handbook on Violence in Education: Forms, Factors, and Preventions* (1st ed.). John Wiley & Sons, Inc. https://www.wiley.com/en-us/The+Wiley+Handbook+on+Violence+in+Education%3A+Forms%2C+Factors%2C+and+Preventions-p-9781118966679

Cornell, D. G. (2020a). *Overview of the Comprehensive School Threat Assessment Guidelines (CSTAG)*. University of Virginia. https://www.researchgate.net/publication/333894588_Overview_of_the_Comprehensive_School_Threat_Assessment_Guidelines_CSTAG

Cornell, D. G. (2020b). Threat assessment as a school violence prevention strategy. *Criminology and Public Policy*, *19*, 235-252. https://doi.org/10.1111/1745-9133.12471

Cornell, D. G., & Burnette, A. G. (2021). Threat Assessment and Management in K-12 Schools. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 136-148). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0007

Cornell, D. G., & Heilbrun, A. (2016). School-Based Risk Factors, Bullying, and Threat Assessment. In K. Heilbrun (Ed.), *APA Handbook of Psychology and Juvenile Justice*. American Psychological Association. https://www.apa.org/pubs/books/4311521

Cornell, D. G., & Maeng, J. (2017). Statewide Implementation of Threat Assessment in Virginia K-12 Schools. *Contemporary School Psychology*, *22*, 116-124. https://doi.org/10.1007/s40688-017-0146-x

Cornell, D. G., & Warren, E. (2024). School Threat Assessment. In C. Franklin, M. B. Harris, & P. Allen-Meares (Eds.), *The School Services Sourcebook* (3rd ed.) (pp. 416-424). Oxford University Press.

Cornell, D. G., & Williams, F. (2011). Student Threat Assessment as a Strategy to Reduce School Violence. In S. R. Jimerson, A. B. Nickerson, M. J. Mayer, & M. J. Furlong (Eds.), *Handbook of School Violence and School Safety International Research and Practice*. Routledge. https://www.routledgehandbooks.com/doi/10.4324/9780203841372.ch37

Deisinger, E. R. D., & Nolan, J. J. (2021). Threat Assessment and Management in Higher Education: Enhancing the Standard of Practice. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 149-165). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255630550

Dunn, J. (2008). Operations of the LAPD Threat Management Unit. In J. R. Meloy, L. Sheridan, & J. Hoffman (Eds.), *Stalking, Threatening, and Attacking Public Figures: A Psychological and Behavioural Analysis*. Oxford University Press. https://doi.org/10.1093/med:psych/9780195326383.001.0001

Dunn, J. (2013). The Los Angeles Police Department Threat Management Unit. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 285-298). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=300

Ellis, H. B., Miller, A. B., Schouten, R., Agalab, N. Y., & Abdi, S. M. (2022). The Challenge and Promise of a Multidisciplinary Team Response to the Problem of Violent Radicalization. *Terrorism and Political Violence, 34*(7), 1321-1338. https://doi.org/10.1080/09546553.2020.1777988

Fein, R. A., & Vossekuil, B. (1997). *Preventing Assassination: A Monograph. Secret Service Exceptional Case Study Project.* https://www.ojp.gov/pdffiles1/Photocopy/167224NCJRS.pdf

Fiedler, N., Sommer, F., Leuschner, V., & Scheithauer, H. (2019). Student Crisis Prevention in Schools:
The NETWorks Against School Shootings Program (NETWASS) – An Approach Suitable for the Prevention of Violent Extremism? *International Journal of Developmental Science*, *13*, 109-122. https://doi.org/10.3233/DEV-190283

Gibson, K. (2023). Pathway to targeted violence: can early intervention work? *Department of Justice Journal of Federal Law and Practice*, *71*(2), 39-76.

Gill, P., & Marchment, Z. (2020). *Further Development of Risk Assessment Schemes for Channel*. Prepared for the Home Office and Centre for Research and Evidence on Security Threats, Lancaster University.

Guldimann, A., Brunner, R., Schmid, H., & Habermeyer, E. (2016). Supporting Threat Management with Forensic Expert Knowledge: Protecting Public Officials and Private Individuals. *Behavioral Sciences and the Law*, *34*, 645–659. https://doi.org/10.1002/bsl.2254

Harris, A. J., & Lurigio, A. J. (2012). Threat Assessment and Law Enforcement Practice. *Journal of Police Crisis Negotiations*, *12*(1), 51-68. https://doi.org/10.1080/15332586.2012.645375

Heitt, M. C., & Tamburo, M. B. (2005). The Development and Evaluation of an Internal Workplace Violence Risk assessment Protocol - One organization's experience. *International Journal of Emergency Mental Health*, *7*(3), 219-226. Chevron Publishing. https://pubmed.ncbi.nlm.nih.gov/16265978/

Holbrook, C. M., Bixler, D. E., Rugala, E. A., & Casteel, C. (2019). The Employee Assistance Program (EAP) and Its Role in the Management of Workplace Threats. In C. M. Holbrook, D. E. Bixler, E. A. Rugala, & C. Casteel (Eds.), *Workplace Violence: Issues in Threat Assessment*. Routledge.

James, D. V., Farnham, F. R., & Wilson, S. P. (2013). The Fixated Threat Assessment Centre: Implementing a Joint Policing and Psychiatric Approach to Risk Assessment and Management in Public Figure Threat Cases. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 299-320). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=314

Kropp, P. R., & Cook, A. N. (2021). Intimate Partner Violence, Stalking, and Femicide. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 189-209). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255630838

Kurutz, J. G., Johnson, D. L., & Sugden, B. W. (1996). The United States Postal Service Employee Assistance Program: A Multifaceted Approach to Workplace Violence Prevention. In G. R. VandenBos, & E. Q. Bulatao (Eds.), *Violence on the Job: Identifying Risks and Developing Solutions*. American Psychological Association. https://doi.org/10.1037/10215-000

Leuschner, V., Bondü, R., Schoer-Hippel, M., Panno, J., NeuMetzler, K., Fisch, S., Scholl, J., & Scheithauer, H. (2011). Prevention of homicidal violence in schools in Germany: The Berlin Leaking Project and the Networks Against School Shootings Project (NETWASS). *New Directions for Youth Development*, *2011*(129), 61-78. **https://doi-org.libproxy.ucl.ac.uk/10.1002/yd.387**

Leuschner, V., Schoer-Hippel, M., Bondü, R., & Scheithauer, H. (2013). Indicated Prevention of Severe Targeted School Violence: NETWorks Against School Shootings (NETWASS). In N. Böckler, T., Seeger, P. Sitzer, & W. Heitmeyer (Eds.), *School Shootings: International Research, Case Studies, and Concepts for Prevention*. Springer-Verlag. https://link-springer-com.libproxy.ucl.ac.uk/book/10.1007/978-1-4614-5526-4

Lloyd, M. (2021). Making Sense of Terrorist Violence and Building Psychological Expertise. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 624-638). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255633901

MacKenzie, R. D., & James, D. V. (2011). Management and Treatment of Stalkers: Problems, Options, and Solutions. *Behavioral Sciences and the Law*, *25*, 220-239. https://doi.org/10.1002/bsl.980

Maxey, W. (2002). The San Diego Stalking Strike Force: A Multi-Disciplinary Approach to Assessing and Managing Stalking and Threat Cases. *Journal of Threat Assessment*, *2*(1), 43-53.

McEwan, T. E., MacKenzie, R. D., & McCarthy, J. (2013). The Problem Behavior Program: Threat Assessment and Management in Community Forensic Mental Health. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 360-374). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=375

McEwan, T. E., & Darjee, R. (2021). The Problem Behaviour Program: Threat Assessment and Management in a Community Forensic Mental Health Context. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 536-553). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0031

Meloy, J. R., Hart, S. D., & Hoffman, J. (2013). Threat Assessment and Threat Management. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 3-17). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=18

Meloy, J. R., & Hoffman, J. (2013). *International Handbook of Threat Assessment* (1st ed.). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/detail.action?docID=1573156

Meloy, J. R., & Hoffman, J. (2021). *International Handbook of Threat Assessment* (2nd ed). Oxford University Press. https://doi-org.libproxy.ucl.ac.uk/10.1093/med-psych/9780190940164.001.0001

Meloy, J. R., Hoffmann, J., Deisinger, E. R. D., & Hart, S. D. (2021). Threat Assessment and Threat Management. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat*

Assessment (2nd ed.) (pp. 3-21). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=18

Meloy, J. R., Hoffman, J., Guldimann, A., & James, D. (2012). The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology. *Behavioral Sciences and the Law*, *30*, 256-279. https://doi.org/10.1002/bsl.999

Meloy, J. R., & O'Toole, M. E. (2011). The Concept of Leakage in Threat Assessment. *Behavioral Sciences and the Law*, *29*, 513-527. https://doi.org/10.1002/bsl.986

Mitchell, M., & Palk, G. (2016). Traversing the Space between Threats and Violence: A Review of Threat Assessment Guidelines. *Psychiatry, Psychology and Law*, *23*(6), 863-871. http://dx.doi.org/10.1080/13218719.2016.1164638

Mohandie, K., & Hoffmann, J. (2021). International Legal Perspectives on Threat Assessment. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 345-359). Oxford University Press. https://doi-org.libproxy.ucl.ac.uk/10.1093/med-psych/9780190940164.003.0019

Mrad, D. F., Hanigan, A. J. S., & Bateman, J. R. (2015). A Model of Service and Training: Threat Assessment on a Community College Campus. *Psychological Services*, *12*(1), 16-19. http://dx.doi.org/10.1037/a0037202

O'Toole, M. E. (2000). The School Shooter: A Threat Assessment Perspective. Federal Bureau of Investigation. https://www.fbi.gov/file-repository/stats-services-publications-school-shooter-school-shooter/view

O'Toole, M. E. (2021). Fundamentals of Threat Assessment for Beginners. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 332-344). Oxford University Press. https://doi-org.libproxy.ucl.ac.uk/10.1093/med-psych/9780190940164.003.0018

Pathé, M. T., Haworth, D. J., Goodwin, T., Holman, A. G., Amos, S. J., Winterbourne, P., & Day, L. (2018). Establishing a joint agency response to the threat of lone-actor grievance-fuelled violence. *The Journal of Forensic Psychiatry & Psychology*, *29*(1), 37-52. https://doi.org/10.1080/14789949.2017.1335762

Phillips, R. T. M. (2008). Preventing Assassination: Psychiatric Consultation to the United States Secret Service. In J. R. Meloy, L. Sheridan, & J. Hoffman (Eds.), *Stalking, Threatening, and Attacking Public Figures: A Psychological and Behavioural Analysis*. Oxford University Press. https://doi.org/10.1093/med:psych/9780195326383.001.0001

Randazzo, M. R., & Cameron, J. K. (2012). From Presidential Protection to Campus Security: A Brief History of Threat Assessment in North American Schools and Colleges. *Journal of College Student Psychotherapy*, *26*, 277-290. https://doi.org/10.1080/87568225.2012.711146

Rappaport, N., Pollack, W. S., Flaherty, L. T., Schwartz, S. E. O., & McMickens, C. (2015). Safety Assessment in Schools: Beyond Risk: The Role of Child Psychiatrists and Other Mental

Health Professionals. *Child and Adolescent Psychiatric Clinics of North America*, *24*, 277-289. http://dx.doi.org/10.1016/j.chc.2014.11.001

Reddy, M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., & Modzeleski, W. (2001). Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches. *Psychology in the Schools*, *38*(2), 157-172. https://doi.org/10.1002/pits.1007

Root, D. A., & Ziska, M. D. (1996). Violence Prevention During Corporate Downsizing: The Use of a People Team as Context for the Critical Incident Team. In G. R. VandenBos, & E. Q. Bulatao (Eds.), *Violence on the Job: Identifying Risks and Developing Solutions*. American Psychological Association. https://doi.org/10.1037/10215-000

Rutz, S. (2021). Mitigating Harm in the Military: A Military Service Approach to Threat Assessment and Management. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 612-623). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0033

Ryan-Arredondo, K., Renouf, K., Egyed, C., Doxey, M., Dobbins, M., Sanchez, S., & Rakowitz, B. (2001). Threats of violence in schools- The Dallas Independent School District's response. *Psychology in the Schools*, *38*(2), 185-196. https://doi.org/10.1002/pits.1009

Scalora, M. J. (2021). Electronic Threats and Harassment: A Dominant Role in Threat Assessment. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 268-282). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255631323

Scalora, M. J., & Racionero, R. V. (2021). Successful Development of Threat Assessment and Management Programming Within a Midwestern University. In K. Heilbrun, H. J. Wright, C. Giallella, & David DeMatteo (Eds.), *University and Public Behavioral Health Organization Collaboration in Justice Contexts: Models for Success*. Oxford University Press. https://doi.org/10.1093/med-psych/9780190052850.001.0001

Scalora, M. J., Zimmerman, W. J., & Wells, D. J. (2008). Use of Threat Assessment for the Protection of the United States Congress. In J. R. Meloy, L. Sheridan, & J. Hoffman (Eds.), *Stalking, Threatening, and Attacking Public Figures: A Psychological and Behavioural Analysis*. Oxford University Press. https://doi.org/10.1093/med:psych/9780195326383.001.0001

Simons, A., & Tunkel, R. F. (2013). The Assessment of Anonymous Threatening Communications. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 195-213). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=210

Simons, A., & Tunkel, R. F. (2021). The Assessment of Anonymous Threatening Communications. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 235-256). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0012

Tobin, C., & Palarea, R. E. (2021). Protective Intelligence: Threat Assessment and Management Considerations. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 360-373). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255631930

Van der Meer, B. B. (2021). Source Interviewing in a Threat Management Context. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 68-83). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255629965

Van der Meer, B. B., & Diekhuis, M. L. (2013). Collecting and Assessing Information for Threat Assessment. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 54-66). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=69

Van Dreal, J., & Okada, D. (2021). A Review of the Working Dynamics of the Salem- Keizer/Cascade Student Threat Assessment and Willamette Valley Adult Threat Advisory Team Models. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 654-668). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0036

Van Dyke, R., Ryan-Arredondo, K., & Rakowitz, B., & Torres, J. L. (2004). The Dallas Independent School District's Threat Assessment Procedures: Summary of Findings after Four Years of Implementation. In M. J. Furlong, Bates, M. P., Smith, & Kingery, P. M. (Eds.), *Appraisal and prediction of school violence: Methods, issues, and contexts*. Nova Science Publishers, Inc.

Van Dyke, R. B., & Schroeder, J. L. (2006). Implementation of the Dallas Threat of Violence Risk Assessment. In M. J. Furlong, & S. R. Jimerson (Eds.), *The Handbook of School Violence and School Safety: From Research to Practice*. Lawrence Erlbaum Associates

Van Horn, D. (2013). Threat Assessment in the U.S. Navy and Marine Corps. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (1st ed.) (pp. 375-387). Oxford University Press. https://ebookcentral.proquest.com/lib/ucl/reader.action?docID=1573156&ppg=390

Vossekuil, B., Fein, R. A., Berglund, J. M. (2015). Threat Assessment: Assessing the Risk of Targeted Violence. *Journal of Threat Assessment and Management*, *2*(3-4), 243-254. http://dx.doi.org/10.1037/tam0000055

Vossekuil, B., Fein, R. A., Reddy, M., Borum, R., & Modzeleski, W. (2004). *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*. United States Secret Service and United States Department of Education. https://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf

Warren, L. J., MacKenzie, R., Mullen, P. E., & Ogloff, J. R. P. (2005). The Problem Behavior Model: The Development of a Stalkers Clinic and a Threateners Clinic. *Behavioural Sciences and the Law, 23*, 387-397. https://doi.org/10.1002/bsl.593

White, S. G. (2021). Workplace Targeted Violence: Assessment and Management in Dynamic Contexts. In J. R. Meloy & J. Hoffmann (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 107-135). Oxford University Press. https://academic-oup-com.libproxy.ucl.ac.uk/book/30016/chapter/255630278

Wilson, S. P., Pathé, M. T., Farnham, F. R., & James, D. V. (2021). The Fixated Threat Assessment Centers: The Joint Policing and Psychiatric Approach to Risk Assessment and Management in Cases of Public Figure Threat and Lone Actor Grievance-Fueled Violence. In J. R. Meloy, & J. Hoffman (Eds.), *International Handbook of Threat Assessment* (2nd ed.) (pp. 471-487). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0027