5-1-2024

Threat and Risk Assessment Measurement: A State of the Science Review

Sam T. Hunter
Katherine Parsons
Kelsey Ciagala
Sydney L. Reichin
Matt Allen

See next page for additional authors

Follow this and additional works at: https://digitalcommons.unomaha.edu/ncitereportsresearch
Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE
Authors
Sam T. Hunter, Katherine Parsons, Kelsey Ciagala, Sydney L. Reichin, Matt Allen, Erin M. Kearns, Austin C. Doctor, and Joel Elson
Threat & Risk Assessment Measurement: A State of the Science Review

National Counterterrorism, Innovation, Technology, and Education (NCITE) Center of Excellence

May 1, 2024

NCITE Research Team
Sam Hunter – University of Nebraska Omaha, NCITE Center
Katherine Parsons – University of Nebraska Omaha, NCITE Center
Kelsey Ciagala – University of Nebraska Omaha, NCITE Center
Sydney Reichin – University of Nebraska Omaha, NCITE Center
Matt Allen – University of Nebraska Omaha, NCITE Center
Erin Kearns – University of Nebraska Omaha, NCITE Center
Austin Doctor – University of Nebraska Omaha, NCITE Center
Joel Elson – University of Nebraska Omaha, NCITE Center

NCITE Support Team
Sara Vetter – University of Nebraska Omaha, NCITE Center
Blake Ursch – University of Nebraska Omaha, NCITE Center

NCITE Director
Gina Ligon – University of Nebraska Omaha
**About NCITE.** The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science & Technology Office of University Programs, NCITE is the trusted DHS academic consortium of more than 50 researchers at partner institutions across the U.S. and Europe. Headquartered at the University of Nebraska at Omaha, NCITE is a leading U.S. academic partner for counterterrorism research, technology, and workforce development.

**Acknowledgment.** 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 & Technology Directorate, or the University of Nebraska System.
Table of Contents

EXECUTIVE SUMMARY ......................................................................................................................... 8

KEY THEMES AND LESSONS LEARNED ON THREAT ASSESSMENT .................................................. 9

Overview .............................................................................................................................................. 9

(1) Test Efficacy of Threat & Risk Assessment Tools – Cause for Tempered Optimism ....................... 10
(2) Structured Professional Judgment (SPJ) Tools – Useful but Varied in Use Cases ......................... 11
(3) Training – A Consistent and Sizable Barrier to Entry .................................................................. 11
(4) Buyin – Managing Tensions around Threat and Risk Assessment Use Cases ............................... 12
(5) Siloes – The Persistent Barrier to Advancing Threat & Risk Assessment .................................... 12
(6) Learning from Allies, Local and Abroad – Lessons, but No Silver Bullets ................................. 13
(7) Insider Threats – The Need to Better Integrate Internal and External Lenses ............................. 13
(8) Novel Threats – Why it is So Challenging to Identify Emerging Threats .................................... 14
(9) In Practice – The Reality of Threat/Risk Assessment is, Counterproductively Disorganized ........ 15

Promising Practices and Future Directions ......................................................................................... 15

Concluding comments ....................................................................................................................... 16

A Focus on Test Efficacy ....................................................................................................................... 18

Introduction .......................................................................................................................................... 19

Definitional Debates Should Not Slow Progress ............................................................................... 20

Threat and Risk Assessment Instruments Can Help Predictions ......................................................... 21

Threat and Risk Assessment Instruments Appear Applicable to Many ............................................ 23

Threat and Risk Assessment Performance is Moderated by Several Design Features .................... 23

  Factor 1: Risk Factor Types.................................................................................................................. 23
  Factor 2: Data Inputs ............................................................................................................................. 24
  Factor 3: Tool Genesis ......................................................................................................................... 24
  Factor 4: Authorship Bias .................................................................................................................... 25

Blending Insights from Different Instruments can Improve Predictive Accuracy ............................ 25

Prediction is not Everything ................................................................................................................ 26

Assessments Require Multivariate Explanations of Risk ................................................................. 27

Implications for Threat/Risk Assessment for Targeted Violence .................................................... 29

  Definitional Debates Should Not Slow Progress .............................................................................. 29
  Risk Assessment Instruments Can Help Predictions ......................................................................... 29
  Risk Assessment Instruments Appear Applicable to Many ............................................................. 30
  Risk Assessment Performance Can be Moderated by Several Design Features ............................ 30
  Blending Insights from Different Instruments Can Improve Predictive Accuracy ......................... 31
  Prediction is not Everything ............................................................................................................... 31
  Assessments Require Multivariate Explanations of Risk ............................................................... 32

Conclusion ........................................................................................................................................... 32

Appendix 1 ........................................................................................................................................... 33

Threat Assessment Practices in the Field ............................................................................................. 36
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>37</td>
</tr>
<tr>
<td>Introduction</td>
<td>38</td>
</tr>
<tr>
<td>Sample and Data Collection</td>
<td>38</td>
</tr>
<tr>
<td>Method</td>
<td>39</td>
</tr>
<tr>
<td>Auto-Coded Themes</td>
<td>39</td>
</tr>
<tr>
<td>Manual Coding</td>
<td>40</td>
</tr>
<tr>
<td>Sentiment Analysis</td>
<td>40</td>
</tr>
<tr>
<td>Findings and Analysis</td>
<td>41</td>
</tr>
<tr>
<td>Finding 1: Background and pathways to threat assessment work</td>
<td>41</td>
</tr>
<tr>
<td>Finding 2: Training issues</td>
<td>43</td>
</tr>
<tr>
<td>Finding 3: Tool Use</td>
<td>44</td>
</tr>
<tr>
<td>Finding 4: Variability in Tool Coverage</td>
<td>45</td>
</tr>
<tr>
<td>Finding 5: Program Development Challenges</td>
<td>46</td>
</tr>
<tr>
<td>Finding 6: Variability in Organizational Approaches</td>
<td>46</td>
</tr>
<tr>
<td>Finding 7: Variability in Individual Approaches (individual beliefs)</td>
<td>47</td>
</tr>
<tr>
<td>Finding 8: Issues and Challenges are a Part of Threat Assessment Work</td>
<td>47</td>
</tr>
<tr>
<td>Findings 9a and 9b: Insider and Novel Threats</td>
<td>48</td>
</tr>
<tr>
<td>Supplemental Findings: Sentiment analysis</td>
<td>49</td>
</tr>
<tr>
<td>Limitations around Generalization</td>
<td>50</td>
</tr>
<tr>
<td>CONCLUSIONS</td>
<td>50</td>
</tr>
<tr>
<td>The State of the Evidence</td>
<td>52</td>
</tr>
<tr>
<td>Introduction</td>
<td>53</td>
</tr>
<tr>
<td>Effects (has it worked?)</td>
<td>54</td>
</tr>
<tr>
<td>Mechanisms (how did it work?)</td>
<td>55</td>
</tr>
<tr>
<td>Moderators (what conditions are needed for it to work?)</td>
<td>56</td>
</tr>
<tr>
<td>Implementation (what was needed to be put in place?)</td>
<td>57</td>
</tr>
<tr>
<td>Economics (is it cost effective?)</td>
<td>59</td>
</tr>
<tr>
<td>Supplemental Reports: Blind Spots in Threat &amp; Risk Assessment</td>
<td>60</td>
</tr>
<tr>
<td>Blind Spot A: Removing Domestic Fixation by Turning to Lessons from Our International Partners</td>
<td>61</td>
</tr>
<tr>
<td>The State of the Evidence ii</td>
<td>62</td>
</tr>
<tr>
<td>A Directory of Threat Assessment Models</td>
<td>63</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>63</td>
</tr>
<tr>
<td>Introduction</td>
<td>63</td>
</tr>
<tr>
<td>Methodology</td>
<td>67</td>
</tr>
<tr>
<td>Inclusion criteria</td>
<td>67</td>
</tr>
<tr>
<td>Search strategy</td>
<td>67</td>
</tr>
<tr>
<td>Included Studies</td>
<td>68</td>
</tr>
<tr>
<td>Threat assessment models</td>
<td>72</td>
</tr>
<tr>
<td>Schools</td>
<td>72</td>
</tr>
<tr>
<td>Dallas Threat of Violence Risk Assessment</td>
<td>76</td>
</tr>
</tbody>
</table>

Supplemental Reports: Blind Spots in Threat & Risk Assessment

Blind Spot A: Removing Domestic Fixation by Turning to Lessons from Our International Partners
Methods .......................................................................................................................... 154
  Focus Groups Notes ....................................................................................................... 154
  Analysis ....................................................................................................................... 154
Findings and Analysis ..................................................................................................... 158
  Finding 1: Collaboration is Key .................................................................................... 158
  Finding 2: Community matters a great deal ............................................................... 158
  Finding 3: Current events prompt progress ................................................................ 159
  Finding 4: Funding discrepancies .............................................................................. 159
  Finding 5: Barriers are diverse .................................................................................... 159
  Finding 6: Structured Professional Judgment Tools (SPJs) ......................................... 160
  Finding 7: Insider threats are on the radar at the local level-at least for some .......... 161
Supplemental Findings: Autocoded Themes .................................................................. 161
Limitations Around Generalization .............................................................................. 161
Law Enforcement Interviews and Survey Instrument .................................................. 162
  Survey Sample ........................................................................................................... 162
  Survey Instrument ....................................................................................................... 162
Findings .......................................................................................................................... 162
  Threat Reporting Systems .......................................................................................... 162
  What is Missing from Reports? ................................................................................... 163
  Recommendations for System Improvement ............................................................. 163
Conclusions ..................................................................................................................... 165
  Communications and Collaboration ........................................................................... 165
  The Community ........................................................................................................ 166
  Takeaways .................................................................................................................. 166
Blind Spot C: Reducing External Threat Fixation – A Necessary Refocusing on Insider Threat .................................................. 168
A Review and Integration .............................................................................................. 169
Introduction ....................................................................................................................... 170
  Part 1: Insider Threat Literature Review ................................................................. 172
  Part 2: Literature Related to Insider Threat ............................................................. 172
  Part 1: Insider Threat Literature Review .................................................................. 172
  Defining Insider Threats ............................................................................................ 173
  Models of Insider Threat .......................................................................................... 174
  Methods for Detecting Insider Threats ...................................................................... 176
  Key Takeaways from Part 1 ...................................................................................... 177
  Part 2: Literature Related to Insider Threat ................................................................ 180
  Practitioner-Oriented Resources .............................................................................. 180
  Social and Behavioral Science Perspectives ............................................................. 190
  Key Takeaways from Part 2 ...................................................................................... 200
Conclusions and Next Steps .......................................................................................... 201
  Future Part 3: Building Predictive Models of Workplace Violence, Espionage, and Sabotage .............................................................. 201
  Future Part 4: Prevention-Focused Solutions ............................................................. 202
Blind Spot D: Mitigating Threat Fixation – The Unique and Harmful Impact of Novelty on Threat Assessment .......................................................... 203
Overcoming a Bias Against Novelty in the Evaluation of Threats ................................................................. 204
Introduction .................................................................................................................................................. 205
Resistance to Novelty: Unpacking the Originality Bias ............................................................................ 208
  Novel Threat Characteristics .................................................................................................................... 208
  Evaluator Characteristics ....................................................................................................................... 210
  Context Characteristics .......................................................................................................................... 211
  Lessons from Organizational Psychology and Management ............................................................. 213
  Applying Lessons to Future Research Directions ................................................................................ 218
SUMMARY STATEMENT AND CONCLUDING COMMENTS .................................................................... 221
References .................................................................................................................................................. 223
EXECUTIVE SUMMARY

Threat and risk assessment are the processes of identifying, assessing, and managing threats of targeted violence prompted by warning behaviors. Threat assessment differs from the traditional operations of law enforcement as it may provide predictive information rather than investigating threats after a violent offense has been committed. Threat and risk assessment examines the escalation of behavior over time and corroborates information from multiple sources to reach a level of concern. Initially developed as a way to prevent assassinations, the tools and approaches around threat assessment have emerged as a violence prevention measure in many settings, including workplaces, schools, universities, and even private corporations. Due to its increasing and ubiquitous use, it is necessary to critically examine the effectiveness of such methods and models in preventing violent and harmful events.

The National Counterterrorism Innovation, Technology, and Education (NCITE) Center at the University of Nebraska Omaha was tasked to examine the current state and promising practices of threat assessment and threat management programs by the Department of Homeland Security. More specifically, this effort seeks to evaluate current programs to better understand the need, utilization, and efficacy of these tools and models. This objective was met via three deliverables. An examination of 23 meta-analyses, comprising 2,108 individual studies that include more than 1 million participants, the Threat/Risk Assessment Literature Review provides a comprehensive framing of what threat and risk assessment entails, the effectiveness of these assessments, and the potential implications of these assessments at preventing or mitigating targeted violence. Threat Assessment Interviews: Threat Assessment Practices in the Field provides a more detailed understanding of how threat and risk assessment professionals are using these tools in their day-to-day work along with any challenges that may impact the tools’ effectiveness. Lastly, What Works in Threat and Risk Assessment, for Whom, and in What Circumstances? The State of the Evidence acts as a supplementary document to the overall Threat/Risk Assessment Literature Review. This document examines if these tools have worked, how they worked, what conditions are needed for success, what needs to be implemented, and the cost of using these tools.

Additionally, through this effort, four “blind spots” of current threat assessment models and practices were discovered that may impact the accuracy and effectiveness of their use.

These blind spots include:

- A fixation on domestic methods and procedures
- A fixation on threat assessment and management at the federal level
- A fixation on external threats while overlooking potential insider threats
- A fixation on common or frequent threats while overlooking novel threats

Five reports were developed to help bring attention to these blind spots and provide guidance on how to remove and address these fixations.

Two reports were aimed at removing a fixation on domestic methods. A Directory of Threat Assessment Models provides detailed information on 27 existing threat assessment models. Models developed in the United States, Germany, the United Kingdom, Switzerland, Australia, and the Netherlands are included. A short deliverable entitled Threat Assessment Models: Lessons from Abroad goes above just exploring the various models but also discusses four important lessons learned from allies abroad.
The purpose of the Threat Assessment Team Focus Groups report was to help shed light on the threat assessment practices at the local level, addressing federal-level fixation. The main objectives of this paper were to identify promising practices from the local level that might apply at the federal level and to assist in the facilitation of communication between federal and local level authorities by observing potential avenues for connection.

As most threat assessment models and practices focus on external threats, many of these models may miss important threats posed by insiders. The paper Examining Best Practices in Threat Assessment from an Insider Threat Perspective: A Review and Integration was developed to bring attention to insider threats and remove a fixation on external threats. This deliverable uses a variety of different literature to highlight what an insider threat is, why insider threats may be important to explore from a threat assessment perspective and key takeaways that can assist researchers and practitioners alike.

To remove the fixation on common or frequent threats, the paper Overcoming a Bias Against Novelty in the Evaluation of Threats explores the phenomenon that individuals tend to favor familiar and prototypical behavior, ideas, and products. This report explores the originality bias, why novel threats might be overlooked, and provides information on how to combat these biases using organizational psychology and management literature.

In all, these reports serve to explore the current state of threat assessment models and management within the United States, providing important insights for improving our current practices. This synthesis continues as follows. First, we will discuss the overarching themes, conclusions, and lessons learned across the entirety of the research project. That is, we discuss the major themes and lessons from across all of the various reports included below to consolidate and synthesize the overarching conclusions. These takeaways represent the cumulation of the entire research project. We then address lessons learned from each of the major pillars included in the research project. Finally, we offer guidance on promising practices in threat assessment and future directions for managers and scholars.

The conclusions begin with takeaways from the primary task to test the efficacy of threat and risk assessment tools, including the efficacy and utilization of Structured Professional Judgment (SPJ) tools. We then discuss some of the primary barriers facing practitioners that emerged throughout the project—namely, those surrounding training, obtaining buy-in, and the siloed nature of threat assessment. Following this, we outline overarching findings from the insider threat space and across our research regarding novel threat preparation and originality bias. Finally, our findings regarding the real-world application and administration of threat assessment practices are presented.

Following this overview, we provide each of the individual research reports from across the period of performance, in order of completion. Further, we offer a brief conclusion and next steps for improving threat assessment practices in a variety of spaces for both practitioners and researchers.

**KEY THEMES AND LESSONS LEARNED ON THREAT ASSESSMENT**

**Overview**

The primary goal of this project was to better understand the psychometric properties (e.g., reliability and validity) of the current threat assessment and threat management tools used by a variety of different professionals across various sectors. Although there was notable variability across tools, is that threat and risk assessment tools are – in the aggregate – effective and psychometrically sound. Through interviews with practitioners as well as a review of the academic literature, however, we also identified
several areas of concern which we referred to as “blind spots” in the threat assessment space. Importantly, we believe that addressing these blind spots will improve the effectiveness and usefulness of these threat assessment and threat management tools. In total, seven different reports explored the primary research directive. We offer the major takeaways and lessons learned from this collective effort, below.

(1) Test Efficacy of Threat & Risk Assessment Tools – Cause for Tempered Optimism

Overall, evidence supports the usage of threat and risk assessment instruments to gain, maintain, or understand the current risks and threats in a variety of contexts. Specially, researchers at the University College London in partnership with NCITE offered seven major takeaways observed in a systematic review of these tools:

- Definitional debates should not slow progress.
- Risk assessment instruments can help predictions.
- Risk assessment instruments appear applicable to many.
- Risk assessment performance can be moderated by several design features.
- Blending insights from different instruments can improve predictive accuracy.
- Prediction is not everything.
- Assessments require multivariate explanations of risk.

Interviews with practitioners who are familiar with threat assessment and who use threat assessment in their work supported these conclusions along with drawing attention to important areas that were not discussed as fully in the academic literature. For example, while the literature review suggested the use of structured professional judgment methods, practitioners also cited them as their preferred method for conducting risk/threat assessments. Additionally, while these tools may be reliable and valid, training issues can prevent practitioners from accessing them or using them properly. Overall, buy-in from relevant others and the siloed nature of threat assessment as a practice may also hinder its effectiveness in practical settings. Beyond the effectiveness of the tools and how they are used, the literature review and practitioner interviews revealed potential threats that are missing from measurement: insider threats and novel threats. Each of these major findings and areas of potential improvement are further discussed in more detail.

One note on the first point offered by the UCL team is the issue of unnecessary contention in the academic literature. Namely, issues around definitions and labels are, in and of themselves, a cause for siloed thinking, in turn producing a territorial terrain that pushes scholars into individual “camps” rather than identifying the commonalities among constructs and methods. In particular, the use of the term threat assessment and risk assessment are viewed by many not as synonyms or largely overlapping terms, but rather as wholly distinct phenomena. This debate is well summarized by Melloy and Hoffman (2021) and we encourage the reader to examine this area for an excellent historical summary of why the divide occurs. We offer, however, that some degree of definitional debate is healthy for the field as clear operationalization is necessary for valid measurement. Scholars and practitioners should seek to identify areas of commonality rather than division. Although we concede differences, we generally see the dividing line between the two not as substantive division, but rather as emphasis and application.
(2) Structured Professional Judgment (SPJ) Tools – Useful but Varied in Use Cases

As stated previously, a major component of the threat assessment space currently is the use of SPJs for assisting in threat assessment. Through our research, we have found reassuring, albeit tempered, multivariate data about the validity of these tools. It is critical to keep in mind when assessing validity that validity exists on a continuum, with a range of validity types (e.g., content, construct, convergent, discriminant, ecological, face) contributing to the broad decision about the validity of a given tool or technique. More directly, criterion-related validity is not the only form of validity and, in fact, is likely to be less useful in low-base rate areas of investigation such as terrorism. This is compounded by the fact that when tools are used to intervene in a threat or risk assessment case, they should – by design – limit the occurrence of violent outcomes, further decreasing information relevance in assessing validity. This is not to say these tools would lack predictive validity in a higher base rate context, but rather that predictive validity should be viewed as the primary means of assessing the validity of SPJ tools for reasons outlined above.

Although SPJ tools have evidenced reasonable validity, particularly when viewed in a multivariate context, we have also learned some lessons about their usage in practice from a range of practitioners. SPJs are a useful tool in the threat assessment professional’s “toolbox” as there is ample evidence of their utility for threat assessment. However, it is important to note that the variation of tool usage across different practitioner spaces was surprising. We discovered that while many teams have adopted SPJs in their assessment practices, they utilize them at different points in the process and at times for different threat assessment goals. While tools are often intended as guidance for decision-making on cases that have escalated to them, in practice, SPJs are used for a range of decision-making processes. For example, we found that some teams utilize SPJs as a form of a “check” on their in-house threat assessment, to verify that the team has covered all bases, so to speak. Some teams utilize SPJs as a form of triaging; that is, they use the assessment output of various SPJs to determine if a case is worthy of a full threat assessment, or whether to discard the case instead. Further, multiple practitioner teams identified SPJs as a means of obtaining buy-in from related parties regarding threat management. That is, some found it easier to obtain approval and support from leadership if they were able to demonstrate the output of an SPJ assessment aligned with their own.

Evident from this observation is that, while tools are generally designed for a specific component of threat assessment, their use, in practice, varies widely regarding the objective and temporal order of assessment. It is unclear how these differences in practice impact the reliability and validity of this process for threat assessment. More research is needed to fully understand if or how temporal differences or differences in intended use can impact threat assessment efficacy.

(3) Training – A Consistent and Sizable Barrier to Entry

A third theme to emerge in this work was the issue of training. Typically, many threat assessment tools and techniques require some level of training, which is often provided in some form (i.e., virtually, in-person training, applied training sessions, and so on) from the creator of the tool itself and is often expensive. The cost is more problematic for smaller teams or organizations where just one individual is tasked with threat assessment. Interestingly, training was not only seen as a barrier from a cost perspective; it was perceived to be a barrier simply due to time and personnel restrictions. Many practitioners are required to perform a variety of different tasks – threat assessment is just one such task that may be infrequently done. Across our interviews, many participants cited the problem with receiving one-time training for tools that are used infrequently.
While training is certainly an issue for threat assessment professionals, it cannot be resolved with funding alone. Rather, effective training could include tabletop exercises, where the tool is practiced regularly by those involved in threat assessment. In addition, training should be ongoing, so that assessors stay sharp with their tool usage and apply them as intended.

In addition to the funding barrier to training, the personnel restrictions related to training are also important to address. Finding and maintaining the right people (those who are invested and believe in the threat assessment approach) is crucial, especially in organizations where threat assessment is only one component of their functions. Teams of all sizes should regularly conduct tabletop exercises, to maintain their skills in between assessments. Further, recruitment into threat assessment teams should be intentional and targeted, seeking those who believe in the approach and function of threat assessment and, especially, SPJs. This finding relates directly to our next theme, which was present across all of the various research streams included in this project.

(4) Buy-in – Managing Tensions around Threat and Risk Assessment Use Cases

A fourth theme of our work was that of buy-in, or gaining commitment and belief to a given effort from a range of participants. This finding illuminates one of the biggest takeaways across the various deliverables–buy-in is crucial for effective threat assessment. From a criminal justice perspective, law enforcement traditionally strives for an arrest or some form of official intervention. However, threat assessment is an approach that typically attempts to support practices that mitigate a threat and prevent the need for an arrest. At its core, for law enforcement especially, this approach is contrary to their training and their real-world experiences.

Issues around buyin may include a commitment from auxiliary figures, leaders, law enforcement, and crucially, those engaged in threat assessment practices directly. Importantly, these groups may have different reasons for supporting or not supporting the threat assessment process. At the leadership level, buy-in of the threat assessment process is crucial for implementing threat assessment within an organization initially, but also, for understanding the unique needs of threat assessment professionals. Some leadership buy-in issues may include budget, personnel constraints, lack of knowledge, and/or lack of awareness. At other times, there is a lack of buy-in by the law enforcement tasked with collecting data for SPJs or assessments more generally.

Education about the methods, goals, and evidence backing threat assessment processes in general and SPJs in particular can help improve buy-in across all points of the threat assessment process. Buyin is more than just education, however—many professionals we interacted with cited “needing the right people,” suggesting that those in threat assessment should come into the practice with an open mind, regardless of their professional background.

(5) Siloes – The Persistent Barrier to Advancing Threat & Risk Assessment

Similar to buyin, another identified theme of this work was the barrier-like role that siloes play in limiting information exchange. More directly, the siloed nature of threat assessment (be they agency, disciplinary, federal vs. local, country) significantly hampers the spread of threat assessment practices and may hinder its overall effectiveness. These siloes manifest both within organizations and across areas of research. For example, silos are particularly prevalent with practices surrounding insider threat detection and management. This is, in part, due to the history of insider threat mitigation being situated in counterespionage efforts, as well as the increased reliance on Information Systems & Technology (IS&T). This has resulted in the majority of insider threat mitigation efforts being situated within the IS&T departments of many organizations, often removed from whatever threat assessment efforts are
underway. It was found that some threat assessment teams are removed from the organizations they are assigned to protect. This is a problem as the most successful teams are those that incorporate other members of the organization, such as those in Human Resources (HR) and managers, into the threat assessment process. This allows for better information sharing, a consistent referral process, and management that can extend beyond the threat assessment itself.

This sort of holistic approach is widely cited by practitioners as crucial to effective threat assessment team management. In addition to taking an organization-wide approach, the most effective teams are also interdisciplinary, including expertise from multiple disciplines. For example, some successful teams include clinical psychologists in addition to law enforcement, legal representatives, and other representatives from the organization. This helps overcome the silos that exist in the academic literature, by allowing each discipline a seat at the table.

(6) Learning from Allies, Local and Abroad – Lessons, but No Silver Bullets
Across two reports, we turned from a focus on normative approaches at the U.S. federal level, to what threat professionals do both abroad and at the local level (i.e., state and local law enforcement). Lessons unique to our allies in the U.K. included the use of softer language to engage as many individuals as possible and not escalate threats simply through language alone. Our allies also tend to take a more holistic approach to threat and risk assessment, considering a wider range of factors than is done in the U.S. There is also greater proactiveness in identifying cases of concern. That is, rather than deciding if a given individual represents a threat, professionals will engage with that individual when more minimal signs emerge. This results in a more supportive context that can mitigate threats before a formal assessment is needed. Finally, our allies abroad as well as at the state and local law enforcement levels stressed the importance of collaboration and community. Using diverse teams of experts to offset blind spots was critical, as was communicating clearly, respectfully, and often.

These lessons are useful and provide meaningful guidelines on ways to improve threat assessment management and measurement in the U.S. Although these lessons are useful, there were a few highly surprising or counterintuitive observations made across these efforts. Instead, they represent a series of small lessons that, in the aggregate, offer a substantive path to improve threat assessment domestically.

(7) Insider Threats – The Need to Better Integrate Internal and External Lenses
We also observed that the aforementioned siloes are especially prevalent in the insider threat space. In multiple instances, we discovered that insider threats were handled by entirely separate groups than an organization’s threat assessment team, oftentimes in the IS&T space. This is prevalent in the academic literature as well. Many of the existing mitigation efforts are situated in IS&T, resulting in automated screening and access control that at times results in a reactive rather than preventive framework. That is to say, detecting inappropriate access only discovers malicious behavior after it has begun, potentially missing important preventive management strategies, such as focusing on protective factors.

In addition, workplace violence, while on the rise in the United States (Van Dam, 2023), is often not conceptualized as a component of insider threat. In fact, in some SME interviews, we were told that workplace violence is simply not a component of insider threats and is not in their wheelhouse. However, by following the integrated, holistic, interdisciplinary approach outlined above, we can manage any type of threat, rather than parceling out insiders exclusively to the tech department. These efforts are important and crucial for an effective security framework within any organization.

Further, the nature of threat assessment within an organization can have implications for efficacy and compliance. That is, the framing of threat assessment is an important component of existing efforts.
some instances, teams have chosen to rename themselves, such as at the University of Nebraska Omaha, where NCITE is situated. The newly renamed Campus Assessment, Response, and Evaluation Team (CARE Team) “serves as the coordinating hub of a network of existing resources and focuses on prevention and early intervention in campus situations involving students experiencing distress or engaging in harmful or disruptive behaviors” (UNO CARE Team, n.d.). Prior, it was referred to as the “Behavioral Response Team.” Anecdotes suggest this change has been highly effective, with dramatic increases in reporting and engagement.

The terminology around threat assessment can be off-putting to some and can impact buy-in and cooperation more generally. However, calling an assessment team a CARES team or akin provides a message of concern and outreach. While these are generally goals of traditional threat assessment teams, in practice, the framing of “threat” assessment has a negative connotation that can impact both cooperation with assessment and management, as well as buy-in. The framing, implementation, and orientation of similar programs and teams within organizations should be conducted mindfully, with this framing in mind. This extends beyond the naming of teams or programs, to the implementation as well. As new measures are introduced, intentional practices should be outlined to involved parties such as employees to avoid the potential for unintended consequences and improve buy-in more generally (Ciagala, et al., 2024). However, it is important to note this finding applies to public-facing framing, rather than academic or policy approaches.

(8) Novel Threats – Why it is So Challenging to Identify Emerging Threats

An additional key theme emerging from the collective efforts of this project was around the observation that novel threats are more likely to be dismissed due to their novelty. The originality bias is a term scholars use to describe how individuals favor what is familiar and prototypical, often rejecting unique ideas (Hunter et al., 2022; Licuanan et al., 2007; Mueller et al., 2012; 2014). This poses a problem for many in the workplace but particularly challenges the homeland security workforce. For those responsible for assessing and prioritizing threats, this can lead even experienced experts to overlook new dangers (e.g., new threats, that we have not previously seen). For example, the attacks on 9/11 introduced a novel type of attack through the hijacking of a large passenger airline. Although we now have practices in place to prevent such an attack, this was outside the scope of what the security workforce was prepared for in 2001. As such, we propose that this originality bias stifles the security workforce’s ability to evaluate potential threats, especially threats that are novel.

One of the main barriers proposed in the evaluation of novel threats is a lack of existing evaluative standards to evaluate the threat. Taken from the idea evaluation literature, evaluators forecast the likely outcomes or consequences of implementing an idea, which often stems from existing standards that exist related to that idea. In other words, decision-makers often rely on their past experiences as a guide, but this is more cognitively demanding when evaluating novel ideas where no such frame of reference exists. Because of these cognitive demands, we posit that novel threats may be ignored. To mitigate this and other barriers to the evaluation of novel threats, we recommend pulling from the organizational sciences, as lessons from leadership, teamwork, organizational climate, and human resource practices may be key to addressing the originality bias in the HSE.

In our practitioner interviews, we found that practitioners tended to adopt the view that, because protective and risk factors are often similar regardless of the nature of the threat, adopting threat assessment practices prepares us for novel attacks and threats more generally. That is, a threat actor is a threat actor, regardless of the attack type, and as a result, novelty is rarely distinguished in any capacity. Stated in perhaps less optimistic terms, practitioners may continue to be biased by novel threats, believing they are equally capable of identifying them when both the academic literature and history provide evidence to the contrary.
(9) In Practice – The Reality of Threat/Risk Assessment is, Counterproductively Disorganized

Threat assessment encompasses a wide range of organizations, both private and public, and practices appear to be trending upward, suggesting more will adopt these methods as part of their security landscape in the future. There are numerous methods, training, certifications, and bodies of academic literature to draw from. However, most threat managers describe having no true starting point when tasked with developing a threat assessment team or department, often having to figure things out for themselves. Many were either tasked with the initial development of a program, or throughout the regular duties “discovered” threat assessment. Whether incorporating SPJs or deciding to take a particular training, managers often describe a lack of a starting point or framework to work with. As a result, there is wide variation in practices, team composition, approach, and management strategies between threat assessment teams and programs.

For example, one team may choose to take a no-contact approach when managing a case, meaning that they never make direct contact with the person receiving an assessment. Other teams, however, will make a point to always incorporate the individual directly into the assessment process. In addition, as we outlined above, there are varying practices in the use of SPJs, including their purpose and the point in the assessment process. In short, there is no consistent foundation available for teams or managers, and instead, they are left to pick and choose what elements of threat assessment are available and make sense for their organization to adopt. This is not only potentially frustrating for practitioners, but it may create problems with the validity of threat assessment tools. Many tools are designed and tested for a specific use and any changes to that method and utilization could lower the method’s efficacy without practitioners even being aware.

This self-guided development process also has implications for other themes identified in this report. First, it may be that it can be difficult to piece together the various elements needed for effective threat assessment within an organization due to the siloing that often occurs. Further, without widespread buy-in or belief in threat assessment practices, finding support for various endeavors, such as recruiting more team members or funding new SPJs and training, is a challenge. While education is an important part of overcoming these potential barriers, consolidating the most promising practices and available resources, including funding opportunities, would be a beneficial first step. However, it is important to note that there may not be a one-size-fits-all approach; with that said, a pooling of practices allows practitioners to make informed decisions about what threat assessment practices to implement, and how to best implement them.

Promising Practices and Future Directions

Threat assessment and management are important to public safety and homeland security, ranging from managing threats in the most rural regions to the most populated metropolitan centers in the country. These tools have the potential to offer critical capabilities for a range of security personnel to prevent and manage threats before an attack occurs. In this report, we reviewed the state of the science of threat assessment measurement, as well as specific focus areas, including insider threat practices, preparation for novel threats, lessons from local law enforcement practices, and lessons from abroad. Overall, our research suggests that risk and threat assessment is a valuable tool in a variety of different contexts. While this is an encouraging finding, our research also indicated that there are many areas where the usage of these tools and methods could be improved.

Regarding improving the usage of threat assessment tools, SPJs were found to be generally considered the gold standard for threat assessment by practitioners. Concerningly, when, how, and why this
method was used varied greatly in practice. That is, the same tool may be used at different points in the assessment process by different teams. In addition, the same tools may be used for different purposes. That is, some teams reported utilizing SPJs to triage cases, whereas others used SPJs on the back end of their assessment, as a “check” on their judgment. Unfortunately, many team leaders report having no guidance or framework to base team development upon, which may result in the wide range of practices and approaches observed. This has important implications for future tool development and training as researchers must begin to incorporate the realities of tool use into the design and development of these tools. More research is needed to understand how temporal effects (i.e., when a tool is used in the process) may impact the efficacy of the management system. Additionally, more guidance should be given to practitioners on the proper procedures for the wide variety of risk/threat assessment tools and methods available.

The need for applied and reoccurring training was a theme that came up across multiple areas of this project. Proper training of any method or tool is critical to its proper usage. Without the proper training, errors and inaccurate conclusions are more likely to occur which can have detrimental impacts for preventing and mitigating threats. There were two main issues surrounding training that were discovered: cost prohibitions and labor. Many training programs can be extremely costly, which can prohibit smaller or resource-constrained organizations from taking advantage of them. Additionally, many formal training courses require travel to a specific off-site location. This is not only a potential cost barrier, but many practitioners indicated a lack of availability to do so. Regarding labor and labor requirements, many professionals indicated that they were not part of a full-time threat assessment team. Rather, many practitioners are tasked to complete risk/threat assessment sporadically or on an as-needed basis. Many only received training once, and with the infrequent use of the tools, reported the need for more consistent and periodic training. Making training more cost effective may allow smaller organizations the chance to provide the crucial training needed for the proper use of the tools and methods needed. Additionally, more cost-effective training may make periodic refresher training more accessible. This could allow both small and large organizations to provide frequent training to teams who may use threat assessment techniques less often, keeping their skills and confidence in the method up to date when they are needed.

The issues surrounding training were deeply tied to another theme that came up across the review—the importance of buy-in into threat assessment practices. Buy-in was found to be important for everyone who has the potential to be impacted by its usage, be it colleagues, leaders, or the community in which they are situated. Given the importance of having the “right” people involved (that is, those who believe in the goals and approach of threat assessment) and the importance of an informed and engaged community in reporting cases and assisting with data collection, it is clear that education surrounding both the efficacy and purpose of threat assessment for both assessors and the public are an important component of effective threat assessment in practice.

Concluding comments
The most effective threat assessment teams are those that take a whole-of-organization approach (e.g., incorporate all levels of an organization) and include a diverse, interdisciplinary, and interagency team. In addition, they have support from leadership and trust from their community. Ideally, this approach incorporates IT efforts at insider threat management as well. Finally, they will have a baseline framework upon which to build the team. While there is no “one size fits all” solution, some standardization of practices will be helpful moving forward, especially as more organizations adopt threat assessment practices.
Future SPJ development should expressly consider at what point in the threat assessment process the tool should be used. For example, scholars and practitioners should fully consider the range of realistic applications such as whether a tool is designed to triage cases, decide on allocating substantive resources, or justify current resources allocated to a threat. Further, training associated with SPJs can take steps to overcome some of the barriers we encountered during this research. Namely, training should be iterative and ongoing—that is, training should not be “one and done,” and instead should include ongoing education. In addition, as practice makes perfect, training should incorporate table tops and other forms of applied practice, which is especially helpful for teams that have minimal caseloads and are thus, therefore, less likely to have opportunities to actively apply their knowledge base. In this way, we can help keep training “current,” which may also serve to provide more consistency in practice.
Evaluating Current Threat Assessments and Threat Management Tools:
A Focus on Test Efficacy

NCITE Consortium Research Team
Paul Gill – University College London
Zoe Marchment – University College London
Amber Seaward – University College London
Introduction

Risk assessment and management are core components of policing, intelligence, judicial, and clinical settings. Risk assessment considers available information and determines an individual’s offending risk. Risk management acts to gain or maintain control of the risk posed. Although historically associated with judgments related to the risk of violence recidivism, risk assessment, and management principles increasingly are applied to other types of violence (e.g., stalking) as well as newly emergent criminal ventures with high harm potential (e.g., cybercrime).

Its principles (rebadged as threat assessment and management) are also increasingly used in the pre-crime space where they address those who are deemed ‘at-risk’ of crossing the threshold into offending. This is evidenced by PREVENT in the U.K. counterterrorism infrastructure (and its recent various offshoots in strategies focusing on preventing engagement in cybercrime and serious organized crime). These can be individuals who have engaged with extremist materials or settings and have demonstrated attitudinal affinity with an extremist cause but have yet to mobilize to violence. In the United Kingdom, 4,915 such referrals were made to counterterrorism policing between April 2020 and March 2021. Approximately 14% of these referrals were taken seriously enough for interventions to be implemented to manage their risk.

Plainly speaking, scrutiny of the effectiveness and quality of counterterrorism threat/risk assessment and management come to the forefront when terrorist attacks occur. Unfortunately, this has been too common an occurrence. According to Europol, 2019 witnessed 119 foiled, failed, and completed terrorist attacks from a range of ideological influences across 13 EU Member States. Many recent attackers were known to intelligence services, had previously been closed cases, or had spent time in prison for terrorist offenses. This naturally raises issues about how these individuals were risk-assessed and managed at all points in their trajectory toward offending. Similar concerns have also been evoked about the procedures in place for preventing recent high-profile acts of targeted violence such as mass public murders, school shootings, and workplace violence.

As governments face further budget constraints in a world recovering from the COVID pandemic, the onus on threat/risk assessment and management will likely amplify and necessitate better links across practitioner agencies (both policing and non-), academia, and industry. This is particularly so for those crime types that are both on the increase and have the potential for high harm, be it physical, psychological, or economic. Consequently, there has been a boom in the availability of threat/risk assessment and management instruments over the past decade focused on forms of targeted violence, particularly terrorism. Some were designed by government entities for in-house work, others are commercially available.

Given both the emergent growing demand and nascent supply of these instruments focused on targeted violence, it is worth taking stock of the more voluminous literature on general violence threat/risk assessment and management. We ask: what works, for whom, and in what contexts? We conducted an umbrella review that synthesizes the results of 23 meta-analyses of threat/risk assessment instruments. These meta-analyses collectively cover over 2108 empirical studies on over 1.3 million individuals. Our umbrella review leads us to the following 7 conclusions which we elaborate upon in turn in the sections that follow:

1. Definitional debates should not slow progress
2. Risk assessment instruments can help predictions
3. Risk assessment instruments appear applicable to many
4. Risk assessment performance can be moderated by several design features
5. Blending insights from different instruments can improve predictive accuracy
6. Prediction is not everything
7. Assessments require multivariate explanations of risk

**Definitional Debates Should Not Slow Progress**
Definitional debates regarding what constitutes terrorism are long-standing, context-dependent, and majorly differ across different strands of research. This has the potential to stunt progress in threat/risk assessment research and practice because the contours of what demarcates (a) terrorist engagement from disengagement, (b) radicalization from deradicalization, and (c) reengagement from recidivism, remain so contested. However, this is not a new problem. Gill et al.’s (2021) umbrella review of predictors of violent recidivism demonstrates this is also true for the general violent recidivism literature which means it is surmountable (Table 1).

**Table 1. Recidivism Definitions in Different Meta-Analyses**

<table>
<thead>
<tr>
<th>Study</th>
<th>Parole Violations</th>
<th>Rearrest/ Re-offense</th>
<th>New Charges</th>
<th>Reconviction</th>
<th>Reincarceration</th>
<th>Recommitment to Psych Facility</th>
<th>Treatment Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asscher et al. (2011)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bonta &amp; Blais (2014)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doherty &amp; Bersani (2018)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eher et al. (2016)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eisenberg et al. (2019)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geerlings et al. (2020)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gerhold et al. (2007)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Golenkov et al. (2014)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hanson &amp; Bussiere (1998)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hanson &amp; Morton-Bourgion (2005)</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kreis et al. (2014)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maille et al. (2011)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McCann &amp; Lussier (2008)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mohr_Jensen &amp; Steinhausen (2016)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Olver et al. (2014)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Olver et al. (2011)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Threat and Risk Assessment Instruments Can Help Predictions
A common goal of all risk assessment instruments is to help an assessor grasp what level of risk is currently posed by the individual under assessment. But how accurate are different risk assessment instruments at prediction? Because risk assessment instruments are not designed equally, we should expect a great deal of variability in performance.

A common method of testing the degree to which an instrument can discriminate between those who conduct the outcome of interest (e.g., violent recidivism) from those who do not (e.g., the non-recidivists), is to use Area Under the Curve (AUC). The result determines the probability that a randomly selected, in this case, violent recidivist, was scored highly by the instrument. AUC ROC (Receiver Operating Characteristic) scores of .5 mean complete chance prediction (e.g., tossing a coin would be just as good), between .64 and .7 mean average predictive ability, between .7 and .8 means good predictive ability, .8 to .9 means excellent and above .9 outstanding.

The below table highlights the aggregated predictive performance (as measured by AUC) of a range of instruments across 18 meta-analyses.

### Table 2. Aggregated Predictive Performance of Risk Assessment Instruments

<table>
<thead>
<tr>
<th>Study</th>
<th>Instrument</th>
<th>Recidivism Type</th>
<th>Sample Specifics</th>
<th>AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Babchishin et al.(2012)</td>
<td>Static-99R</td>
<td>Sexual Violence</td>
<td>Sex Offenders</td>
<td>.684</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.703</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any</td>
<td></td>
<td>.718</td>
</tr>
<tr>
<td></td>
<td>RRASOR</td>
<td>Sexual Violence</td>
<td></td>
<td>.661</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.614</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any Recidivism</td>
<td></td>
<td>.582</td>
</tr>
<tr>
<td></td>
<td>STATIC 2002R</td>
<td>Sexual Violence</td>
<td></td>
<td>.686</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.708</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any Recidivism</td>
<td></td>
<td>.732</td>
</tr>
<tr>
<td>Campbell et al.(2009)</td>
<td>HCR 20</td>
<td>Institutional Violence</td>
<td>Adult Offenders</td>
<td>.678</td>
</tr>
<tr>
<td></td>
<td>LSI/LSI-R</td>
<td>General Violence</td>
<td></td>
<td>.642</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutional Violence</td>
<td></td>
<td>.637</td>
</tr>
<tr>
<td></td>
<td>PCL/PCL-R</td>
<td>General Violence</td>
<td></td>
<td>.642</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutional Violence</td>
<td></td>
<td>.585</td>
</tr>
<tr>
<td></td>
<td>PCL: SV</td>
<td>General Violence</td>
<td></td>
<td>.637</td>
</tr>
<tr>
<td></td>
<td>SIR Scale</td>
<td>Institutional Violence</td>
<td></td>
<td>.642</td>
</tr>
<tr>
<td></td>
<td>Vrag</td>
<td>General Violence</td>
<td></td>
<td>.545</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institutional Violence</td>
<td></td>
<td>.637</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.596</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.654</td>
</tr>
<tr>
<td>Viljoen et al.(2012)</td>
<td>JSOAP II</td>
<td>Sexual Violence</td>
<td>Sex Offenders</td>
<td>.670</td>
</tr>
<tr>
<td></td>
<td>ERASOR</td>
<td>General Violence</td>
<td></td>
<td>.660</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual Violence</td>
<td></td>
<td>.660</td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td></td>
<td>.590</td>
</tr>
<tr>
<td>Van Der Put et al.(2019)</td>
<td>All Tools</td>
<td>Domestic Violence</td>
<td>N/A</td>
<td>.647</td>
</tr>
<tr>
<td></td>
<td>CRATP</td>
<td></td>
<td></td>
<td>.760</td>
</tr>
<tr>
<td></td>
<td>DVARAG</td>
<td></td>
<td></td>
<td>.715</td>
</tr>
<tr>
<td></td>
<td>IPPARAT</td>
<td></td>
<td></td>
<td>.780</td>
</tr>
<tr>
<td>Study</td>
<td>Instruments</td>
<td>Offender Type</td>
<td>Score</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------</td>
<td>--------------------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td>.619</td>
<td></td>
</tr>
<tr>
<td>Pusch &amp; Holtfreder (2018)</td>
<td>LSI</td>
<td>Any</td>
<td>.661</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Juvenile Male</td>
<td>.644</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any</td>
<td>.644</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Juvenile Female</td>
<td>.649</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>General Violence</td>
<td>.644</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>YLS</td>
<td>.641</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCL</td>
<td>.695</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NCAR</td>
<td>.603</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OCRA</td>
<td>.585</td>
<td></td>
</tr>
<tr>
<td>Olver et al.(2009)</td>
<td>YA-LSI</td>
<td>Any</td>
<td>.684</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Violent</td>
<td>.678</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent</td>
<td>.666</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual</td>
<td>.608</td>
<td></td>
</tr>
<tr>
<td></td>
<td>YA-PCL</td>
<td>Any</td>
<td>.642</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Violent</td>
<td>.585</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent</td>
<td>.642</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual</td>
<td>.540</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAVRY</td>
<td>Any</td>
<td>.689</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Violent</td>
<td>.719</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent</td>
<td>.678</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual</td>
<td>.534</td>
<td></td>
</tr>
<tr>
<td>Rossdale et al.(2020)</td>
<td>HCR 20</td>
<td>Violent</td>
<td>.679</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any</td>
<td>.642</td>
<td></td>
</tr>
<tr>
<td>Olver et al.(2014)</td>
<td>LSI</td>
<td>Any</td>
<td>.672</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent</td>
<td>.619</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Non-Violent</td>
<td>.642</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual</td>
<td>.579</td>
<td></td>
</tr>
<tr>
<td>O’Shea et al.(2013)</td>
<td>HCR 20</td>
<td>Verbal Aggression</td>
<td>.745</td>
<td></td>
</tr>
<tr>
<td>Helmus et al.(2012)</td>
<td>Static 99R</td>
<td>Sexual</td>
<td>.705</td>
<td></td>
</tr>
<tr>
<td>O’Shea &amp; Dickens (2014)</td>
<td>START</td>
<td>Any Aggression</td>
<td>.714</td>
<td></td>
</tr>
<tr>
<td>Fazel et al.(2012)</td>
<td>8 Tools</td>
<td>Violent</td>
<td>.720</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Tools</td>
<td>Sexual</td>
<td>.740</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Tools</td>
<td>Criminal Offending</td>
<td>.660</td>
<td></td>
</tr>
<tr>
<td>Hanson &amp; Morton-Bourgon (2009)</td>
<td>All Tools</td>
<td>Any</td>
<td>.657</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sexual</td>
<td>.659</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent</td>
<td>.641</td>
<td></td>
</tr>
<tr>
<td>Singh et al.(2011)</td>
<td>SVR20</td>
<td>Any</td>
<td>.780</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SORAG</td>
<td>N/A</td>
<td>.750</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRAG</td>
<td></td>
<td>.740</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAVRY</td>
<td></td>
<td>.710</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HCR</td>
<td></td>
<td>.700</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SARA</td>
<td></td>
<td>.700</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STATIC</td>
<td></td>
<td>.700</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCL</td>
<td></td>
<td>.660</td>
<td></td>
</tr>
<tr>
<td>Tully et al.(2013)</td>
<td>Static 99</td>
<td>Sexual</td>
<td>.692</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RRasor</td>
<td></td>
<td>.668</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SORAG</td>
<td></td>
<td>.684</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RM2000/S</td>
<td></td>
<td>.666</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static 2002</td>
<td></td>
<td>.707</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SVR20</td>
<td></td>
<td>.696</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MnSOST-R</td>
<td></td>
<td>.638</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRS-SO</td>
<td></td>
<td>.755</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRA</td>
<td></td>
<td>.737</td>
<td></td>
</tr>
</tbody>
</table>
We can draw several conclusions from this table. First, the vast majority of meta-analyses place predictive performance in the average-to-good categories, with none performing excellent or outstanding. Therefore, there are limitations to what an instrument can do by itself in terms of prediction.

Second, looking at the crime types listed, the predictive scores tend to err higher for higher base rate outcomes. For example, general violence occurs more often than sexual violence in the general population and those meta-analyses focused on general violence recidivism prediction fare much better. This has major implications for the adoption of threat and risk assessment instruments for types of violence like mass murder and terrorism which have even lesser base rates. However, alternative measures like attitudinal affinity with extremist measures have higher prevalence rates (Wolfowicz et al., 2020) yet attitudes are typically not tested in the broader risk assessment field. A simple cut-and-paste of learning from the assessment of behavior may not be the best route for the assessment of attitudes.

Third, the only demonstration of a meta-analysis looking at the onset of offending compared to recidivism was that of van der Put et al.’s (2019) systematic review of domestic violence prediction. The results showed that those instruments predicting the onset of domestic violence scored significantly higher (AUC = .744) than those predicting domestic violence recurrence (AUC = .643) which points toward the importance of early detection and prevention and the potential of threat assessment instruments to provide capabilities of spotting this trajectory upstream.

**Threat and Risk Assessment Instruments Appear Applicable to Many**

There is good evidence for the wide applicability of risk assessment instruments to different subsets of the population. Some meta-analyses report no gender effects (e.g., instruments performed equally as well for males and females). For example, Pusch & Holtfreder (2018) found no significant difference in performance for males and females on general and violent recidivism. Other meta-analyses report similar for juvenile justice risk assessment instruments (Schwalbe, 2008; Olver et al., 2009), and adult violent risk assessment instruments (Fazel et al., 2012). Only one meta-analysis reported stronger effect sizes for females. Olver et al.’s (2014) meta-analysis found that LSI had stronger performance for females, particularly in terms of general recidivism. The consistent performance of risk assessment instruments across ethnicity (Fazel et al., 2012; Olver et al., 2009) and age (Fazel et al., 2012) has also been demonstrated within meta-analyses.

**Threat and Risk Assessment Performance is Moderated by Several Design Features**

A range of meta-analyses investigated whether the predictive performance of risk assessment instruments is impacted (positively or negatively) by a range of potential moderators. The evidence suggests this is the case in terms of (1) the types of risk factors an instrument contains (2) the types of information that informs an assessment (3) the instrument’s development and risk specification and (4) authorship bias. We look at each in turn.

**Factor 1: Risk Factor Types**

There are different ways of categorizing risk factors, and a popular one is to split them into static and dynamic factors. Static risk factors relate to historical factors that are non-changeable aspects of the person being assessed. Dynamic risk factors relate to situational and other types of stressors that are amenable to change and occur relatively recently to the problem behavior. Campbell et al. (2009)
examined the differential performance of instruments that (1) primarily contain static risk factors (2) dynamic risk factors and (3) an equal combination of static and dynamic risk factors. For institutional violence, static instruments had a significantly larger mean effect than primarily dynamic and mixed instruments. The surprising over-performance of static factors here is likely due to the level of control held, and surveillance maintained, within institutional settings on dynamic risk factors (e.g., access to substances, engagement with third parties). Moving to violence in the community, Campbell et al. (2009) found that for violent recidivism, dynamic instruments performed marginally better than the other two categories. Hanson & Morton-Bourgon (2009) also found instruments containing dynamic factors performed better for sexual violence recidivism prediction than those instruments primarily containing static risk factors. Additionally, in a meta-analysis of a single instrument, the HCR-20, the results demonstrated that the dynamic components of the instrument produced larger effect sizes than the static items when predicting inpatient aggression in forensic settings (O’Shea et al., 2013).

The strong performance of instruments with dynamic risk factors is important because, by definition, dynamic factors are the most amenable to change, and typically form the targets of interventions and management strategies.

**Factor 2: Data Inputs**

Information is crucial to assessments. Depending on the operational context, different types of data sources might inform risk assessments. Some contexts may rely on fully remote assessments with no first-hand contact with the individual being assessed (labeled ‘file review only’). Other contexts might rely solely on first-hand interviews with the individual or solicit self-reports from the individual absent an interview or conduct a mixture of these practices.

Campbell et al. (2009) tested whether the data sources for assessments impacted predictive performance. File review only and a mixture of file review plus interview produced the largest effect sizes for violent recidivism – almost double that of interview only and self-report only. Similarly, Walters’ (2006) meta-analysis demonstrated that combining data sources (in this case file review, interview, and self-report) added incremental validity to predictions compared to relying on a sole source. Schwalbe (2007) demonstrated that ‘file review only’ and ‘direct interview only’ performed just as well as each other for juvenile justice risk assessment instruments but did not compare these with a mixture of the two.

The takeaway from this is that assessments will only be as good as the variety of data sources informing them. Some sources may more readily hold insights into particular factors than others and different sources must offset the potential biases generated from alternative sources. It may not always be possible to interview an individual under assessment (e.g., consent was not obtained, or the assessment is part of a covert investigation), but assessors should try to consider offense paralleling behaviors (e.g. behaviors that are functionally similar to the risk outcome) as well as the risk outcome under consideration to get a more holistic understanding.

**Factor 3: Tool Genesis**

Campbell et al. (2009) also distinguished risk assessment instruments between those that were derived from criminological theory and/or were created primarily as a risk assessment instrument and those that were neither (e.g., instruments focused on issues such as personality, literacy, and self-esteem) but are used to predict violence outcomes. The former, expectedly, performed significantly better at predicting institutional violence and violent recidivism.
Singh et al.’s (2011) meta-analysis of 9 different risk assessment instruments consistently showed that instruments designed for specific populations produced higher rates of predictive validity than more generally oriented instruments. More specifically, Hanson and Morton-Bourgoin’s (2009) meta-analysis similarly showed that risk assessment instruments designed specifically to assess the risk of sexual recidivism performed significantly better than instruments designed for violent recidivism when used to predict sexual recidivism. The inverse was also true, whereby sexual violence risk assessment instruments struggled with predicting violence recidivism compared to those tools designed to assess its likelihood. Van den Berg et al.’s (2018) meta-analysis showed that instruments designed for sexual recidivism risk performed significantly greater for predicting sexual risk compared to violent risk. Olver et al. (2009) conducted a meta-analysis of three risk assessment instruments not designed for sexual recidivism. The LSI was developed to assess the risk of general recidivism, the PCL is a diagnostic tool to reliably measure the presence of psychopathic features, and the SAVRY was designed to assess the risk of violence. For each instrument, performance was significantly greater in predicting general, non-violent, and violent recidivism compared to predicting sexual recidivism. In the case of SAVRY, the effect sizes were five times smaller for sexual recidivism, and in the case of PCL, it was two to three times smaller. However, van der Put et al.’s (2019) meta-analysis of domestic violence risk assessment demonstrated that those instruments developed specifically for domestic violence performed just as well as other more generic violence risk assessment instruments.

The take-home points therefore are that violence risk assessment instruments perform better than psychometric scales, and that risk assessment instruments typically perform best when built specifically for a certain crime type and deployed against that crime type.

**Factor 4: Authorship Bias**

Singh et al.’s (2013) meta-analysis of nine risk assessment instruments demonstrated a significant authorship effect on studies validating these instruments. Average effect sizes were significantly higher when instrument designers were involved in a validation study. Singh et al. (2013) proposed two alternative explanations. First, the result may be incidental. Designers will be more familiar with the instrument, and those working with the designer may more prodigiously stick to the instrument’s guidelines thus producing a greater effect. Second, designers may be more likely to not submit studies for publication that show poor instrument performance. Either way, the effect size differential is so large that all designers should formally declare their engagement in the study and the potential for authorship bias to have occurred.

**Blending Insights from Different Instruments can Improve Predictive Accuracy**

As previously mentioned, there is no shortage of violent extremism threat/risk assessment instruments available (e.g., ERG 22+, IVP, MLG, OVEST, VERA 2R, TRAP 18). The same is true for other forms of violence including general violence (HCR 20 v3, BARR-2002R, VRAG, COVR, VRS, SAPROF, SAVRY), domestic violence (SARA v3, DASH, DVI, ODARA, BSAFER), sexual violence (SVR 20 v2, RSVP, ERASOR, J-SOAP II, PROFESOR, VASOR 2), and stalking (SRP, SAM). It naturally leads to questions about which instrument is best. If we judge ‘best’ naively by predictive validity, then there is no clear answer when there are two or more well-designed instruments. Because each instrument tends to draw on a similar gene pool of scientific evidence, often the items they include can be definitionally similar, thus leading to a high level of correlation between the outcomes generated. For example, O’Shea and Dickens’ (2014) systematic review found multiple studies demonstrating positive correlations between the START instrument with SAPROF, PCR:SV, and individual domains of the HCR-20. Viljoen et al.’s (2012) meta-
analysis found a correlation between four sex-offending risk assessment instruments also (J-SOAPII, ERASOR, JSORRAT-II, and Static-99). Olver et al.’s (2009) meta-analysis of the performance of LSI, PCL, and SAVRY in youth samples similarly shows negligible differences in the performance between these instruments when applied to the same samples.

By synthesizing the results of 20 studies that used three actuarial sex offender risk assessment instruments, Babchishin et al. (2012) investigated whether combining risk scales improved performance. The meta-analysis showed that each scale consistently positively contributed to each other’s performance when predicting recidivism. Van den Berg et al. (2018) replicated this finding in their meta-analysis of dynamic sex-offending risk assessment instruments. Babchishin et al. (2012) also considered what is the most efficient process to consider multiple scales (e.g., take the highest, take the lowest, or average). The analysis demonstrated it was better to average the risk ratings than to consistently choose the instrument that generated the highest score for an individual case. The combination of multiple instruments therefore managed to negate the risk of underestimating and overestimating the risk of recidivism from case to case.

There are potential grounds therefore to make use of multiple instruments in a single assessment, but assessors should have a thorough understanding of the different domains of risk/protective factors incorporated into different instruments and how this may relate to the outcome of interest.

**Prediction is not Everything**

There are three approaches to risk assessment: ‘unstructured’, ‘actuarial’, and ‘structured professional judgment’. Whereas the latter two require risk assessment instruments, the former sees practitioners rely solely on judgment. The identification of characteristics would be based on previous experience, the practitioner’s memory of previous empirical findings, and perhaps intuition (Hilton et al., 2006). This method has proven to be less accurate than assessment based on empirical evidence (Monahan, 2008). Meta-analyses have shown poor predictive performance for such unstructured approaches (Hanson & Morton-Bourgon, 2009), with effect sizes between two to five times smaller than alternative approaches (documented below).

If the practitioner uses the actuarial method, the characteristic chosen will be based on empirical evidence from follow-up studies that identify the relationship of the characteristics to the outcome (Hilton et al., 2006). In this manner, the actuarial method differs from the clinical, as it uses statistics to identify the most powerful predictors of offending. However, this can only be done with outcomes that have an extensive and robust scientific basis underpinning them.

Despite the reported success of using actuarial approaches to risk assessment, some note the potential pitfalls of strictly following statistical results (Douglas et al., 1999; Douglas et al., 2005; Dvoskin et al., 2001). Among these are the difficulty of generalizability beyond the samples used in the development of the tool, the challenge of applying statistical knowledge to a clinical setting, the propensity of actuarial methods to exclude potentially important risk factors, the rigidity of actuarial models, and their lack of space for change. Most importantly, actuarial methods fail to address prevention and risk management.

The combination of statistical methods and clinical judgment methods resulted in a new type of risk assessment, namely the structured professional judgment (SPJ) approach (Douglas & Kropp, 2002; Douglas et al., 2003). SPJ allows practitioners to review all available clinical data to identify any potential risk factors, which are found in a structured manual based on empirical evidence (Douglas et al., 2003). Based on these factors, a final structured risk judgment is made, which indicates the risk of offending (Douglas et al., 2003). Unlike actuarial methods, the SPJ does not include fixed guidelines on
how to calculate the level of risk. Instead, SPJ tools are structured to guide the decision-making process of the practitioners. Tools in this category include a list of risk factors, all of which have been empirically supported, with guidelines on how these risk factors are coded and how to reach a final judgment of different gradations of risk (Douglas et al., 2003).

The major difference between actuarial and SPJ tools is the final risk judgment: actuarial tools only allow for a final decision based on fixed rules and statistical calculations, while SPJ tools allow the professional to make a final decision considering all risk variables that have been identified (Pedersen et al., 2010). Thus, the expertise of the practitioner is still valued, alongside empirical evidence (Douglas et al., 2003).

As Logan and Lloyd (2019:146-147) outline regarding SPJ approaches to violence risk assessment and management:

“The substantial part of SPJ-informed risk assessment and management guidance is the identification of risk factors evidenced in the research as being the most relevant to the specific outcome to be prevented...and the review of evidence justifying their importance...Depending on the guidance [document], support is offered on understanding the relevance of risk factors to the individual case, the meaning of violence to the person at risk, the scenarios in which that violence may become manifest, and risk management planning involving a range of strategies”

SPJ can be completed in an abbreviated form whereby an appraiser identifies risk and protective factors and assigns a rating of high, medium, or low risk “based on the pattern of risk factors present in the case”. This is known as ‘SPJ-lite’. ‘Full’ SPJ, on the other hand, additionally requires scenario planning and formulation (Logan and Lloyd 2019:147).

In terms of predictive performance, Singh et al. (2011) found no difference in predictive performance between actuarial and SPJ instruments across many different outcomes. Fazel (2012) found similar. Van der Put et al.’s (2019) meta-analysis of domestic violence prediction showed actuarial tools fared significantly better. However, the actuarial method has the potential to disregard the different dynamics of risk, including the nature, severity, imminence, duration, and frequency of future offending (Hart, 2001; 2003). So, whilst actuarial methods may aid assessment, they do next to nothing to aid management.

Although prediction is important, the primary purpose of risk assessment should be prevention. This requires a greater understanding of the individual than a straightforward actuarial score can provide. Engaging in violence is a choice. It is carried out with a specific goal, reward, or benefit in mind. The decision might be made quickly, without much forethought, without knowledge of it being an offense, through carelessness or bad (mis)information – but it is still a decision (Hart & Logan, 2011). SPJ focuses on understanding the factors that led to that decision. Why did they cross the threshold into offending? What was happening to the individual at the time (internally and externally) that facilitated or justified the offending? What were the perceived benefits? What goal did they hope to achieve? Were the negative consequences of offending considered? What were the barriers that could have prevented the offending? With these answers, an assessor can draw inferences about the factors that influenced the onset and continued problem behavior, as well as consider the factors that might inhibit further problem behavior.

Assessments Require Multivariate Explanations of Risk

Gill et al. (2021) conducted an umbrella review that synthesized the results of 27 meta-analyses and systematic reviews on predictors of violent recidivism. These 27 evidence syntheses examined at least
526,510 participants and 1,118 primary studies. They found 32 different factors that had been subject to meta-analysis. The below table summarizes their effect sizes and rank orders. Effect size ranges were consistently low ($r < .3$), with only one factor experiencing a range that went into the moderate range ($r = .3-.5$). No individual factor had a high effect size ($r > .5$).

At first, the consistently low effect sizes may appear underwhelming. But the opposite is true. The results demonstrate no single factor will explain the emergence of the risk. The key is to think about multivariate explanations of risk, the interrelationships between risk factors, and their cumulative impact on recidivism likelihood.

Putting gender aside, the strongest effect sizes consistently refer to aspects of personality disorders, prior antisocial/criminal/violent behavior, poor life situations (e.g., living conditions, employment, education), and other factors that impact self-regulation (e.g., substance abuse). On the other hand, socio-demographic characteristics like age, race, and others were amongst the smallest effect sizes.

**Table 3. Meta-analytic factors and effect sizes**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Effect Size from Highest Quality Study</th>
<th>Factor</th>
<th>Effect Size from Highest Quality Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Social Personality Disorder</td>
<td>.44</td>
<td>Substance Abuse (any)</td>
<td>.13</td>
</tr>
<tr>
<td>Personality Disorder (Any)</td>
<td>.29</td>
<td>Personal/ Psychological Problems</td>
<td>.13</td>
</tr>
<tr>
<td>Anti-Social Behaviors</td>
<td>.27</td>
<td>Anti-Social Personality Traits</td>
<td>.13</td>
</tr>
<tr>
<td>Gender (male)</td>
<td>.24</td>
<td>Psychopathic Personality Disorder</td>
<td>.13</td>
</tr>
<tr>
<td>Psychopathic Personality Disorder</td>
<td>.24</td>
<td>Criminal Behavior (previous)</td>
<td>.11</td>
</tr>
<tr>
<td>Living Situation (poor)</td>
<td>.23</td>
<td>Childhood Sexual Abuse Victim</td>
<td>.11</td>
</tr>
<tr>
<td>Alcohol Use</td>
<td>.22</td>
<td>Family Problems</td>
<td>.10</td>
</tr>
<tr>
<td>Violent Behavior (previous)</td>
<td>.21</td>
<td>Relationship Problems</td>
<td>.08</td>
</tr>
<tr>
<td>Employment / Poor Education combined</td>
<td>.20</td>
<td>Married (no)</td>
<td>.06</td>
</tr>
<tr>
<td>Self-Regulation</td>
<td>.18</td>
<td>Race (minority)</td>
<td>.03</td>
</tr>
<tr>
<td>Drug Use</td>
<td>.18</td>
<td>Age (younger)</td>
<td>.01</td>
</tr>
<tr>
<td>Leisure (poor)</td>
<td>.17</td>
<td>Socio-economic status (low)</td>
<td>Non-Significant</td>
</tr>
<tr>
<td>Anti-Social Attitudes</td>
<td>.16</td>
<td>Childhood Physical Abuse Victim</td>
<td>Non-Significant</td>
</tr>
<tr>
<td>Age (older)</td>
<td>.16</td>
<td>Mental Disorder (yes)</td>
<td>Non-Significant</td>
</tr>
<tr>
<td>Criminal Peers</td>
<td>.14</td>
<td>Employment (no)</td>
<td>Non-Significant</td>
</tr>
<tr>
<td>Weapon Use/Threats/ Physical Injuries Caused</td>
<td>.14</td>
<td>Education</td>
<td>Non-Significant</td>
</tr>
</tbody>
</table>

The umbrella review also highlights several areas where evidence is lacking. For example, no meta-analyses examined family criminality, self-esteem, social skills, or social-ecological factors that consider the impact of community dynamics. Only one low-quality design examined the impact of sentence length and did not consider the moderating impact of age. Few studies examined the differential impact of either follow-up periods (e.g., do some risk factors matter more in different follow-up periods) or whether
the index offense involved co-offenders or not. Few meta-analyses considered mediating or moderating effects across studies, and this demonstrates potentially major opportunities for future research.

The definition of risk and protective factors was pretty uniform throughout the evidence syntheses. Simply, studies noted the presence of a factor that has a theoretical or pre-existing empirical correlation with offending and/or recidivism. Often syntheses focused on a single factor like psychopathic traits (Asscher et al., 2011). Studies also simply analyzed whether the presence of a ‘risk factor’ was greater in the violent recidivism group compared to the non-violent recidivism group. There was next to nothing that sought to understand the relevance of a risk factor to the outcome of violent recidivism. This is for two main reasons. First, presence suits idiographic research designs informed by the simple coding that actuarial risk assessment tools produce (e.g., everything coded as yes or no). Relevance is potentially much more suited to qualitative nomothetic research designs which are unsuitable for meta-analyses. Second, SPJ manuals do not have an overt focus on prediction in the same way that actuarial tools do. SPJ assesses and manages, whereas actuarial tools predict. Therefore, actuarial tools and the data they use lend themselves better to meta-analyses. It was surprising that although the HCR-20 is so widely used, we could not find a single meta-analysis that looks at its more nuanced coding scheme for the presence, relevance, and absence of risk factors and their link to violent recidivism.

Implications for Threat/Risk Assessment for Targeted Violence

Definitional Debates Should Not Slow Progress

Transparent and flexible research practices are the key to pushing science forward in this space. For example, consider the grounds for a rigorous violent extremist re-engagement/recidivism study, and set aside the research difficulties associated with its comparatively lower base rate of index offending, and potential difficulty in accessing official data. A major difficulty in such a study would be overcoming the boundary confusion in terms of where re-engagement starts and ends, and when it transitions into violent extremist recidivism. One route to transparency would be to develop a standardized and widely acceptable definition of violent extremism re-engagement and recidivism before any data is collected. Such a definition would articulate inclusion criteria in terms of offending type, and timespan under consideration. From experience, this is likely to be an exhaustive process that is unlikely to achieve the desired consensus that manages to keep all academics and practitioners satisfied. Instead of this exhaustive and likely unsatisfying route, we would suggest a more pragmatic route that prioritizes data collection and flexible definitions. Each small facet of a pre-determined definition has the potential to sway results in any given direction. Instead, a project could list all of the potential facets of a definition and dummy code (e.g., code as yes or no) each one. Rather than checking whether an individual had recidivated against a predetermined definition, coders would answer separately whether there was a parole violation (this is the closest approximation to re-engagement), a rearrest, a re-offense, new charges, reconvictions, reincarcerations, and so on. They could code whether the recidivism was a terrorism offense or not, and whether it occurred within 1, 3, or 5 years, and so on. The outcomes of such a pragmatic datadriven process would show how re-engagement/recidivism rates (and their risk factors) differ according to different definitional permutations.

Risk Assessment Instruments Can Help Predictions

The emphasis here is ‘help.’ Risk assessments are not foolproof because the risk is thoroughly dynamic, subject to ebb and flow, information will be missing or lost between agencies, and there are only finite resources. This message is important for the general public, policymakers, and politicians alike because the expectation is often that 0% risk is the only acceptable outcome in terms of terrorism risk assessment and management. Given the oftentimes more sophisticated, predatory, and crafty behavior
associated with targeted violence versus other forms (which are often impulsive, and substance abuse driven), the expectation that an instrument will provide better results for the former than decades of research have demonstrated for the latter is fanciful. On top of that, risk assessment predictions, generally, work best for high-volume incidents. It was striking to see meta-analyses refer to the somewhat poor performance of sexual violence recidivism prediction as being due to that crime type’s ‘low base rate.’ Compared to targeted violence, it is not a low base rate. So, this again should temper our expectations about prediction and targeted violence.

**Risk Assessment Instruments Appear Applicable to Many**
Decades of research on terrorism and other forms of targeted violence demonstrate there is no single socio-demographic profile. Perpetrators encompass a broad church. Similar performance across gender, age, and ethnicity appears promising for the application of threat/risk assessment instruments to the diverse portfolio of individuals who become radicalized or transition to planning acts of targeted violence.

However, a bigger challenge likely awaits the development and validation of threat/risk assessment instruments in this space. Repeatedly, it has been demonstrated that radicalization and terrorist engagement should be viewed as a process with various discrete phases along the way. These discrete phases depict multiple types of ‘risk’ related to extremism and terrorism. These phases are labeled differently across various theoretical models and include Precht’s (2007) phases of pre-radicalization, conversion and identification, conviction and indoctrination, and action; Borum’s (2003) terrorist mindset model which includes the stages of grievance, injustice, target attribution, and devaluation; Wiktorowicz’s (2004) radicalization model which includes the stages of cognitive opening, religious seeking and frame alignment, socialization and joining; Moghaddam’s (2005) ‘staircase to terrorism’ model involving psychological interpretations of material conditions, perceived options to fight unfair treatment, displacement of aggression, moral engagement, solidification of categorical thinking and the perceived legitimacy of the terrorist organization and the terrorist act and sidestepping inhibitory mechanisms; Silber and Bhatt’s (2007) radicalization model involving pre-radicalization, self-identification, indoctrination, and jihadization. What constitutes a risk factor for vulnerability to radicalization, may not necessarily represent a risk factor for terrorist engagement. Similarly, risk factors may play differential roles at different points of the phases. Threat/risk assessment instruments in this space should therefore be mindful of what phase of the process they are considering the likelihood of harmful outcomes occurring.

**Risk Assessment Performance Can be Moderated by Several Design Features**
*Risk Factor Types:* Traditionally the focus of general violence risk assessment instruments has been on the differential importance of static and dynamic risk factors. This has happened in parallel with the study of radicalization where focus has shifted away from root cause explanations to more group/network-level and dynamic influences. Given the social nature of terrorist engagement, it is likely that additional factors require consideration for this problem area also. Issues related to beliefs and attitudes are often overlooked elsewhere but may relate to the facets of an individual we would typically associate with being radicalized. Social context and capability factors are also often overlooked because of the simple nature of most forms of violence but these factors move closer toward the individual’s immediate social network and capability for violence.
Blending Insights from Different Instruments Can Improve Predictive Accuracy

Existing violent extremism and targeted violence instruments differ in their focus. The risk specifications of some tools vary in focus, such as assessing vulnerability to radicalization (IMV), Jihadist extremist tendencies (EMI), and online radicalization (OVEST). The MLG and TRAP-18 are limited to “group violence” and lone-actor terrorism respectively. Others are slightly broader e.g. ERG (risk of reoffending), and VERA (violent extremism). Table 4 notes the percentage of risk factors for each tool, further demonstrating the different types of focus. It is likely some assessment cases could benefit from multiple instruments being looked at.

Table 4. Distribution of Risk Factor Types by Violent Extremism Instrument

<table>
<thead>
<tr>
<th>Tool</th>
<th>Static Risk Factors</th>
<th>Dynamic Risk Factors</th>
<th>Beliefs, Attitudes, Behavior</th>
<th>Social Context &amp; Capability</th>
<th>Protective Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>IVP</td>
<td>0%</td>
<td>31.25%</td>
<td>25%</td>
<td>43.75%</td>
<td>0%</td>
</tr>
<tr>
<td>EMI</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>OVEST</td>
<td>7.69%</td>
<td>7.69%</td>
<td>30.77%</td>
<td>30.77%</td>
<td>23.07%</td>
</tr>
<tr>
<td>ERG22+</td>
<td>13.67%</td>
<td>4.55%</td>
<td>59.09%</td>
<td>27.27%</td>
<td>0%</td>
</tr>
<tr>
<td>MLG</td>
<td>30.43%</td>
<td>17.39%</td>
<td>21.74%</td>
<td>30.43%</td>
<td>0%</td>
</tr>
<tr>
<td>MLG2</td>
<td>23.81%</td>
<td>19.05%</td>
<td>23.81%</td>
<td>33.33%</td>
<td>0%</td>
</tr>
<tr>
<td>VERA</td>
<td>12.5%</td>
<td>8.33%</td>
<td>37.5%</td>
<td>20.83%</td>
<td>20.83%</td>
</tr>
<tr>
<td>VERA2</td>
<td>13.79%</td>
<td>0%</td>
<td>51.72%</td>
<td>17.24%</td>
<td>17.24%</td>
</tr>
<tr>
<td>TRAP-18</td>
<td>16.66%</td>
<td>27.77%</td>
<td>44.44%</td>
<td>11.11%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Prediction is not Everything

Fortunately for violent extremism threat/risk assessment, prediction is not everything, because the science lags far behind the other forms of violence outlined in the preceding sections. Few instruments here have demonstrated the ability to discriminate between persons of interest and those that are not, few have demonstrated inter-rater reliability and certainly none have been tested to the extent that a meta-analysis is achievable.

Fortunately, SPJ approaches are currently in vogue in this space and widely seen as best practice amongst those who have responsibility for risk assessment in a variety of clinical, forensic, and custodial settings.

Each of the instruments in this space either explicitly or implicitly (e.g., IVP) identifies itself as an SPJ approach. However, the grounds by which they self-identify as SPJ differ. The likes of IVP, EMI, OVEST, and VERA encourage the first two steps of SPJ (e.g., gather information and resources; determine the relevance of factors to individual risk) but fall far short of providing advice on formulation, scenario planning, and management strategies. IVP, for example, provides “useful and relevant information to practitioners about issues they should consider” and encourages decisions being made “in conjunction
with practitioners’ professional judgment and expertise, and consultation with line management and agency policy” (Cole et al., 2010: 2). IVP falls short of providing the full SPJ process of formulation, scenario planning, and management strategies. The ERG22+ goes a step further than IVP and uses formulation but not scenario planning.

The TRAP-18 and MLGs are the closest match in terms of the degree to which they mirror SPJ development guidelines. This is particularly so with the MLG whose developers were also heavily involved with Historical Clinical Risk-20 (HCR-20), the Guidelines for Stalking Assessment and Management (SAM), and other highly rated risk assessment tools for other types of violence. The TRAP-18 manual suggests formulations and management approaches. However, the guidance provided is comparatively very limited, with just 1 page in the guidance document, and appears underdeveloped compared with the MLG.

**Assessments Require Multivariate Explanations of Risk**

Empirical research demonstrates that targeted violence is usually the culmination of a complex mix of personal, political, and social drivers that crystallize at the same time to drive the individual down the path of violent action. Whether the violence comes to fruition is usually a combination of the availability and vulnerability of suitable targets that suit the heady mix of personal and political grievances and the individual’s capability to engage in an attack from both a psychological and technical capability standpoint. Many individual cases share a mixture of unfortunate personal life circumstances coupled with an intensification of beliefs that later developed into engaging in violence. What differed was how these influences were sequenced. Sometimes personal problems led to a susceptibility to ideological influences. Sometimes long-held ideological influences became intensified after the experience of personal problems. This is why we should be wary of mono-causal master narratives. The development of these behaviors is usually far more labyrinthine and dynamic. Threat/risk assessment instruments need to embrace this complexity rather than shy away from it with pre-determined algorithms.

SPJ-informed assessments aim to make sense of an individual’s behavior in the context of their unique circumstances. The ‘risk’ someone poses is subject to change. It is driven by situations and circumstances. This is particularly true for adolescent populations, who are subject to major changes in their lives. An instrument should help assessors determine the nature and degree of risk an individual poses for certain kinds of behavior given their current and future circumstances. By understanding the individual’s trajectory into a problematic behavior, we might gain insight into the factors that might exacerbate or stem the issue. Assessments can inform our understanding of future likely scenarios, and the tailored management plans that are required to avert harm. We need to look at each case on its individual merits by weighing and integrating the evidence and gaining an overall understanding of the individual, their behavior, intentions, and motives. We seek to understand whether there is a risk of harm, its nature, scale, severity, and imminence. Through this, we seek to prevent potentially harmful outcomes. To do so, we require priorities for intervention that guide risk management. Identifying these priorities is contingent on getting a thorough understanding of the individual.

Assessors should not weigh the presence of each risk factor equally. If an individual has a lot of risk factors but little proclivity or skills for seriously harmful cybercrime, the risk is likely low. On the other hand, there might be cases where only one factor is present but is highly influential in driving harmful risk. The purpose here of an instrument should be to help assessors exercise their best judgment.

**Conclusion**

The meta-analyses and systematic reviews we synthesized throughout this paper are overtly focused on the instruments, their psychometric properties, and their predictive capabilities. Yet some hugely
important issues remain curiously overlooked. Behind every risk assessment is an individual practitioner, behind them is an organization, and in front of them are individuals in need of assessment, many requiring some form of intervention. Practitioners will differ in experience, professional background, and degrees of training. Institutions will differ in terms of caseload, supervisory capacity, and data access. Those assessed as ‘high risk’ will likely have greater wraparound interventions which, in theory, should disrupt the onset of offending (and make the overt focus on prediction even more curious). Yet none of these issues are synthesized thus far are likely far more consequential for real-life harm reduction than an instrument’s predictive powers, especially so when low base rate events are the subject of inquiry. Future work on this project will endeavor to do so through a systematic review of the human factors side of risk assessment and management.

Unlike actuarial approaches, SPJ approaches do not include fixed guidelines on how to calculate the level of risk and allow practitioners to review all available evidence to identify any potential risk (or if applicable, protective) factors. SPJ approaches then typically direct a user to code the relevance of an individual indicator. By relevance, we mean the degree to which the item motivates, disinhibits, or destabilizes the risks posed by the individual being assessed (e.g. its functional relation to offending). SPJ then typically involves a generation of a statement of understanding about the case (e.g. a formulation). It is imperative to synthesize the quality of formulations and whether (a) formulation quality impacts on outcomes, (b) formulations conducted remotely differ from those informed by contact with the individual, and (c) training and experience impact the quality of formulations. Additionally, we know very little right now about how risk assessments inform management approaches. Does the presence/volume of risk factors impact subsequent intervention intensity? Are interventions emanating from formulations evidence-based, tailored to the culture and individual characteristics, and do they draw on building protective factors? Questions such as these are paramount for threat/risk assessment and management, particularly for an understanding of what works, for whom, and in what contexts.

Appendix 1

We conducted a keyword search of titles and abstracts in ProQuest and PsycINFO for papers published from database inception until 28th November 2020, restricted by English language. For ProQuest, we used the following databases: PRISMA, Public Health Database Information, Psychology and Social Science Premium Collection. For PsycINFO, we used the following databases: Journals, PsycArticles Full Text, PsycBooks, PsycheXtra, PsycInfo, PsycTests, and Social Policy and Practice.

We used the same keywords for both databases. Key words searched for issues related to recidivism (recidiv* OR re?offen* OR desist* OR re?imprisonment OR re?conviction OR repeat offending OR recur* OR re?arrest OR re?incarceration OR violation OR relapse OR reoccur* OR re?institution* OR setback OR repetit* OR rehabili* OR recall), violence (violenc* OR crim* OR offen* OR antisocial OR delinqui* OR aggress* OR abuse OR conflict OR threat OR harm OR assault OR force OR intent* OR serious bodily harm OR victim OR violation), risk or protective factors (risk OR protect* OR predict* OR moderat* OR mediati* OR need OR factor OR cause OR determinant OR indicator OR explain OR predecessor OR associated OR precede OR impact OR antecedent OR promot*), and publication types (meta* OR systematic review OR rapid evidence assessment OR scoping review OR evidence map OR rapid review OR research synthesis* OR Campbell). We also conducted forward and backward citation searches to supplement the search.

The inclusion criteria sought evidence syntheses on predictors/inhibitors of violent recidivism. For the purposes of the sift, we:
• used the HCR-20’s definition of violence: "Actual, attempted or threatened infliction of bodily harm on another person. Bodily harm includes both physical and serious psychological harm so long as it substantially interferes with the health or well-being of an individual. Psychological harm includes fear of physical injury and other emotional, mental or cognitive consequences of the act in question."
• understood recidivism as a person’s relapse into criminal behavior, often after the person receives sanctions or undergoes intervention for a previous crime.
• defined a risk factor as something that is considered to contribute (directly or indirectly) to the perpetration of violence. This can be specific to the individual, their upbringing, their context, and their experiences.
• broadly defined a protective factor as something that inhibits (directly or by buffering risk factors) the perpetration of violence.
• focused on evidence syntheses such as meta-analyses, and systematic reviews.

For the purpose of the search and sift, we were purposefully broad in the definitions of what constitutes recidivism and what a risk/protective factor for it is. The purpose of this broadness was to give us the ability to flesh out the contours of definitional boundaries across relevant evidence syntheses.

Figure 1 depicts the search process. Four researchers sifted through 2,854 studies and excluded 2,767 for not meeting all of the definitions above, based on an assessment of the title and abstract. 87 full papers were analyzed by one member of the team. 21 were excluded because they were some forms of evaluation on a single type of intervention, not an instrument. 33 were excluded because they solely focused on specific risk factors, not ones that prescriptively belonged to a named risk assessment instrument. 8 were excluded because they did not distinguish violent recidivism from general recidivism, although the abstract suggested otherwise. 2 were excluded because although the abstract was in English, the full paper was not.

---

**Figure 1:** Systematic Search Process & Rates of Attrition
The remaining papers and those identified in the forward citation search were analyzed and key sources of information (e.g. study design features, variables, effect sizes) were extracted by a second member of the team. To allow for a standardized comparison, we converted all Cohen’s $d$, Odds Ratio, Standard Normal Deviate $z$, and Pearson’s Correlation $r$ to Area-under-Curve using one of two online effect size converters (https://www.escal.site, https://www.polyu.edu.hk/mm/effeetsizefaqs/calculator/calculator.html).
Threat Assessment Interviews:
Threat Assessment Practices in the Field

NCITE Center Research Team

Kat Parsons – University of Nebraska at Omaha
Kelsey Ciagala – University of Nebraska at Omaha
Sydney Reichin – University of Nebraska at Omaha
Sam Hunter – University of Nebraska at Omaha
Executive Summary

The National Counterterrorism Innovation, Technology, and Education (NCITE) Center at the University of Nebraska Omaha is currently leading a task to examine best practices in current threat assessment and threat management programs. The primary focus of the current document is to update NCITE’s work around threat assessment tool perceptions and use in the field. Interviews with threat assessment practitioners were conducted to help us gain a deeper understanding of the real-world application of threat assessment tools in the threat management space. We interviewed practitioners from a range of backgrounds who perform threat assessments as a primary part of their work functions.

The objectives of these interviews are to:

1. Gain a core understanding around perceived practitioner utility of threat assessment tools and models (i.e., are current tools any “good” in practice?), and,

2. Gain a core understanding of practical applications of threat assessment tools and models from the perspective of practitioners (i.e., how are current tools actually used, if used at all?).

Given the variety of backgrounds and use cases, interview structures varied, yet each interview made a point to touch on four primary themes: (a) background in threat assessment, (b) tool usage/coverage, (c) insider threats, and (d) novel threats. We interviewed 13 practitioners, including individuals from law enforcement, military, and state/county levels (such as school districts). These interviews, while illuminating, do not represent the full scope of threat assessment work, and should not be interpreted as such. However, these interviews provided several important insights that can help guide our understanding of the real-world application of threat assessment tools, as well as the needs of assessors and future directions.

No personally identifying information was collected on the interviewees, and interviews were not recorded. However, extensive contemporaneous notes were taken during interviews, which served as the basis of this analysis. These notes document every question/response that occurred during the interview, providing a wealth of information. These notes were both manually coded, as well as “auto-coded” using machine learning processes and Natural Language Processing to detect themes and sentiment across the texts. The manual codes were determined from themes identified by the research team conducting the interviews. Manual codes identify themes and relationships across interviews and allowed for an in-depth assessment of our findings across all 13 interviews.

The first major finding concerns the process of developing threat assessment programs within various organizations. That is, regardless of whether a manager we spoke with came from law enforcement, the military, or otherwise, a recurring theme was the lack of a starting point. In short, the starting point for program development is unclear and resulted in managers doing their own research to determine how to develop a program, what to include, and how to practice threat assessment for their purposes. While there is no one-size-fits-all approach to program development, some form of guidelines or standards may facilitate future program development, as well as allow for a more standardized process.

Second, Structured Professional Judgment (SPJ) tools were frequently cited as preferred for threat assessment cases. However, although threat assessment tools are designed for specific applications (for example, the WAVR-21 is designed to assess the risk of targeted violence in the workplace), we found that they were not necessarily being utilized by the same practitioners at the same point in the process. Therefore, while the purpose of the tool may be clear to practitioners, the optimal point in the threat assessment process and attendant circumstances that govern those practices are not always clear to those working in the field.
Finally, a prominent theme in our analysis of the interview notes was training. Issues regarding training in the threat assessment space were not limited to issues regarding access and cost—although these were major concerns. Rather, it was the call for a strong foundation in training that stood out as the most prominent theme across interviews. This involves not only regular training but the need for refresher training, particularly in light of the sometimes scarce use of the assessment tools. That is, training is only useful insofar as the skills learned do not deteriorate over time and can be drawn upon when needed, even when the use of specific tools may only need to be used rarely.

An in-depth report of our data collection, methods, and resulting analysis follows.

Introduction
The primary focus of the document is on updating our work around threat assessment tool perceptions and use in the field. Interviews with threat assessment practitioners were conducted to help us gain a deeper understanding of the real-world application of risk assessment tools in the threat assessment space. We interviewed practitioners from a range of backgrounds who work with threat assessment as a primary part of their work functions.

Sample and Data Collection
Interviews were conducted with practitioners with a range of backgrounds in the threat assessment space, including multiple levels of the military, multiple levels of law enforcement, civilian federal security, and school district security. Interviews were open-ended, but questions were developed around the following criteria:

- Practitioner backgrounds
- Previous threat assessment experience
- Availability, utility, and forms of training and guidance
- Given expertise in threat assessment, suggestions for improvement of tools and approaches
- Current preferred tools (or general approaches)
- Tools used prior that were removed or disregarded
- Reasons/rationale for why some tools are preferred over others
- General perception around tool utility in supporting threat assessment
- How tools are used, practically speaking
- Perceptions of tool utility in helping to identify novel and insider threats
- Perceptions of tool utility for identifying non-external threats
- Are different tools utilized for different stakeholders in differing ways (i.e., variability in application)

We completed 6 interviews with law enforcement entities, 5 across military entities, 1 at the county school board level, and 1 who recently left public service for private consulting, resulting in the final set
of 13 interviews. All contacts were obtained as part of a “snowball” sampling effort that began with a list of contacts from the Department of Homeland Security Science & Technology Directorate (DHS S&T), our partner organization in this research. That is, in addition to the initial contacts provided by DHS, we asked the initial interviewees to provide additional points of contact (i.e., snowballed) to increase the sample of research participants. All interviewee personal information and identifiers have been masked for privacy and safety purposes; however, each interviewee was selected because their day-to-day working operations included the use of threat assessment tools.

While interviews were open-ended, interview questions revolved around four primary themes: (a) background/experience with threat assessment tools, (b) preferred tools, (c) insider threats, and (d) novel threats. Instead of recordings and transcriptions, for privacy protection, we conducted interviews with a contemporaneous note taker, who also served as a researcher on the project. In addition, one senior researcher from the NCITE team conducted the interview, in addition to the note taker. Interviews began in April 2022 and concluded in May 2022, and were all one hour or less.

**Method**

Although interviews were not recorded, extensive contemporaneous notes were taken during each interview. These notes, alongside observations by the researchers who conducted the interviews, provided the basis for this assessment. These sources were analyzed in three stages. First, researchers discussed themes across interviews, identifying three main themes: (a) approaches to threat assessment (individual and organizational), (b) tool coverage/usage, and (c) issues encountered (including in program development, tool usage, and buy-in). In the next stage, these themes were used to manually code each interview line-by-line, with the inclusion of additional codes: insider threats, novel threats, the breakdown of individual vs. organizational program development, and the breakdown of tool usage vs. tool coverage. The codes are outlined in full in Figure 2.

Finally, the interviews were compiled in qualitative analysis software, with each interview serving as a unique case. The software utilized – NVivo – is designed for the qualitative and mixed-methods analysis of unstructured text, such as that from interviews, video, and other sources (Using NVIVO in Qualitative Research, 2020).

**Auto-Coded Themes**

For the first wave of analysis, we utilized NVivo’s auto-coding feature to identify themes across the interviews. During the theme auto-coding process, NVivo...

“...detects significant noun phrases (for example, real estate development) to identify the most frequently occurring themes.

The process collects the themes and counts their mentions across all files in the set being processed.

NVivo actively filters the themes—only the most relevant themes are presented in the results. You can choose which themes to create as nodes at the end of the process.”

(Automatically Detect and Code Themes, n.d.)

**Figure 1.** Auto-coded themes
This feature in part relies on an existing dictionary of omitted—or ‘stop’—words. The stop words dictionary is per language, which was set to English for this project, and includes commonly used words such as “the, and, they” and so on. In addition to the existing standard stop words, stop words of relevance to this project were added, to avoid them being automatically detected and compiled as themes. The additional stop words included for this analysis were: threat assessment, assessment, tool & tools. Because interview questions revolved around these keywords, their inclusion would have biased the theme analysis. It is worth noting that “risk” likely stands out as a top theme for these reasons and should be omitted in any future analyses. The results of the auto-coding of themes in NVivo were compared to the themes identified by the research team. While the themes identified by the team largely aligned with the auto-coding, one additional theme was identified that stood out as a top mention—training. In fact, the issue of training stood out as one of our top themes across all interviews, indicating what a pressing and real-world concern it is to those in the threat assessment space. The results of the auto-coded themes are outlined in Figure 1. While these results are largely to be expected given the topic of the interviews, the prominence of “training” as a theme stood out as that was not one of the themes identified by the research team during the interview phase. As a result, we did a “deep dive” into the conversations around training, which are outlined more extensively later in this report.

**Manual Coding**

In addition to the overarching themes identified initially, the manual coding of the interview notes allows us to make comparisons across interviews and understand any trends and patterns that emerge. Manual codes began with a series of themes identified by the research team during the interview phase. Secondary coding was conducted with the content within these codes to identify subthemes and their relationship to other coding themes. The list of manual codes and subcodes is presented in Figure 2. The hierarchy of code application across interviews are represented in Figure 3.

<table>
<thead>
<tr>
<th>Name</th>
<th>Files</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual approaches</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Tool coverage</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>Organizational Approaches</td>
<td>8</td>
<td>47</td>
</tr>
<tr>
<td>Insider Threats</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td>Novel Threats</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>Training</td>
<td>8</td>
<td>30</td>
</tr>
<tr>
<td>Time</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Strategy</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Cost</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>Foundation</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>Tool usage</td>
<td>9</td>
<td>35</td>
</tr>
<tr>
<td>Individual tools</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>No SPs</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Developed tool</td>
<td>7</td>
<td>33</td>
</tr>
<tr>
<td>Issues Encountered</td>
<td>9</td>
<td>40</td>
</tr>
<tr>
<td>Buy-In</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Suggestions</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>Critiques</td>
<td>8</td>
<td>34</td>
</tr>
<tr>
<td>Background</td>
<td>9</td>
<td>29</td>
</tr>
<tr>
<td>Program development</td>
<td>5</td>
<td>27</td>
</tr>
<tr>
<td>Origin</td>
<td>8</td>
<td>25</td>
</tr>
<tr>
<td>Professional experience</td>
<td>9</td>
<td>31</td>
</tr>
<tr>
<td>Interview Questions</td>
<td>13</td>
<td>160</td>
</tr>
</tbody>
</table>

**Sentiment Analysis**

Sentiment analysis is a Machine Learning process that uses Natural Language Processing (NLP) to automatically detect and code sentiment in text, ranging from Very Negative to Very Positive. NVivo has a built-in Sentiment Analysis function similar to the Theme Coding function—both analyses’ methods utilize machine learning to automatically detect and code text. There are some important limitations to keep in mind when analyzing sentiment analysis results. Sentiment analysis in NVivo functions by searching for expressions of sentiment in the content.

Per NVivo,

“It is important to understand that this tool does not classify content according to sentiment. It does not take each piece of content and rate it on a Likert sentiment scale. It looks at the sentiment of words in isolation—the context is not taken into account.
Like most text analysis tools, NVivo cannot recognize:

- sarcasm
- double negatives
- slang
- dialect variations
- idioms
- ambiguity

(Automatically Detect and Code Sentiment, n.d.)

Despite these limitations, this sentiment analysis function is a way to gain insight into trends regarding sentiment across interviews. That is, it presents a snapshot of the interviewee’s assessment regarding any given topic. In addition, because we utilized contemporaneous notes across interviews, there are limited issues with sarcasm, slang, and so on.

Findings and Analysis

**Finding 1: Background and pathways to threat assessment work**

Background information included professional experience more generally, and specifically, how each interviewee came to work in the threat assessment space. In the second round of manual coding, background information was further coded into three different categories: Professional Experience, Origin, and Program Development. **Professional Experience** refers to the interviewee’s professional experience before and leading up to their work in the threat assessment space, while **Origin** refers to their transition into threat assessment from their previous field. Finally, **Program Development** refers to the process by which interviewees (where applicable) came to design, develop, and implement threat assessment programs at various levels and institutions.

Our interviewees generally took one of three paths into the threat assessment space: law enforcement, military, or behavioral psychology (either as a practicing psychologist or through working with behavioral psychologists). Most notable however was the paths individuals took to develop and implement new threat assessment programs within their organizations. Five of our interviewees were involved in program development in this capacity. Everyone, regardless of whether their background was in law enforcement or the military, described a process of individual research and often, self-discovery regarding the importance and need for behavioral threat assessment in the first place. For example, one respondent described realizing the need and value of threat assessment as a process of “peeling back the layers” when assessing threats and explained that his skillset coalesced to provide the opportunity to engage in this space. Another described the process as “starting in the gray.”

In fact, multiple respondents described a certain element of chance or luck involved in the process. For example, one interviewee in law enforcement described meeting a forensic psychologist in a professional capacity as the turning point in understanding the need for threat assessment. Another attended a conference where they happened to have lunch with a Canadian threat assessment expert. What became clear throughout the interviews was that there was no one path into threat assessment and that
there was also little guidance and few standards to guide leaders in the development of threat assessment programs.

**Figure 4.** Hierarchy Chart of All Manual Codes—the size of the box denotes the frequency of code application across interviews.
Finding 2: Training issues

Training was a top theme identified through the auto-coding process and was raised by the majority of the practitioners we interviewed. In the second phase of manual coding, training was further broken down into five additional categories: Strategy, Time, Cost, Foundation, and Other. Strategy refers to discussions about approaches to training, while Time refers to issues relating to the time involved in participating in threat assessment training. Cost refers to issues relating to the cost of threat assessment training. Foundation refers to issues regarding the need for a strong training foundation in threat assessment, as well as the needs associated with providing that foundation. Finally, Other simply sums up comments on training that did not fit into any other category. One example of a comment that fell into the Other category referred to excitement about the upcoming NTER Master Training to be provided by DHS, and suggesting that DHS-sponsored training on utilizing SPJs for threat assessment would be a crucial “next step” toward increased utilization of behavioral threat assessments in practice.

Figure 5. Training codes by number of references. The size of the box corresponds with the number of times that code was utilized across all interviews. We found that building a strong foundation with training was the most prominent topic regarding training, over even cost.

The National Threat Evaluation and Reporting (NTER) Master Trainer Program (MTP) certifies Federal, State, Local, Tribal, and Territorial (F/SLTT) partners in the instruction of Behavioral Threat Assessment and Management (BTAM) techniques and best practices. This train-the-trainer program prepares Certified Master Trainers to empower their local communities and organizations to mitigate threats and prevent acts of targeted violence. (Master Trainer Program One-Pager / Homeland Security, 2022).

Training stood out as a primary theme across interviews for a number of reasons. First, and perhaps most pressing, are the budgetary concerns regarding training in various threat assessment tools. While many SPJs have formal training that is available to a range of practitioners, it is often very expensive and was frequently cited as a constraint against tool use and adoption. These constraints are further amplified by the number of individuals requiring training (and
can therefore limit the number of available threat assessors), the number of tools training is required for, and the need for refresher training. In short, the need often greatly outweighs the funding available.

This has a series of implications for the use of SJP tools in the threat assessment space. The need for threat assessment tools ranges from small, single-person units responsible for the threat assessment of a finite space, such as a school system, to massive organizations responsible for the threat assessment of entire branches of the military, for example. However, the tools utilized (or the desire to utilize tools) across these spaces are often the same, regardless of organizational size. Further, training tends to be developed and implemented by those responsible for creating a particular tool. For example, the co-creators of the WAVR-21, a commonly utilized tool aimed towards determining the risk of workplace and campus violence, offer regular 2-day training courses in their tool, with the most recent training workshop costing $695 per registrant ($347 for active duty law enforcement officers) (WAVR-21 Training FAQ, n.d.). This is in addition to the cost of purchasing WAVR-21. In short, not only may this be cost-prohibitive for smaller departments, but the larger the need (for example, the need to train 5 assessors vs. 1), the larger the cost. When we add in the need for many, if not most, assessors to utilize multiple tools in their functions, budgetary constraints are a major roadblock in the utilization of SPJs across various spaces and institutions.

Training is not simply an issue involving cost, however. The most prominent concern regarding training was the need for a strong foundation in tool usage. One interviewee described having attended the same training workshop for a particular SPJ tool multiple times, explaining that they learned something new every time they attended. Therefore, training should not be viewed as a “one-and-done” process, but rather, an ongoing one, with refreshers on various instruments being offered regularly, and being another potential cost consideration. Bureaucratic red tape can also be a constraint, especially when access to funding relies on exterior grants and other supplemental funding. Due to these constraints, some assessors we spoke with were unable to use the range of tools they would like or have the team size they felt necessary for their function.

**Finding 3: Tool Use**

Tool use, describing the use (or lack thereof) of either existing or in-house SPJ tools. In the second phase of coding, this was further broken down into: (a) *Developed Tools*, referring to the use of commercial SPJ tools for threat assessment; (b) *Individual Tools*, referring to the development and use of in-house SPJ tools; and finally, (c) *No SPJ*, for those not using SPJ tools in their threat assessment work in any capacity. We found that most were using developed tools to some extent, while only two interviewees were not using SPJ tools in any capacity. In addition, two of those we spoke with were working with in-house developed tools that catered to their particular needs.

*Figure 6. Relationship Between Training and Developed Tool Usage. The arrows represent the direction of the coding relationship, while the numbers designate the number of code intersections across interviews.*
The ways that different tools are utilized in the threat assessment process can vary widely from one organization to the next. At times, the same tool may be used at completely different points in the assessment process by different organizations. While SPJ tools are never supposed to be the entirety of the threat assessment process, it is noteworthy that where one organization may use a particular SPJ to triage cases, another may use that same tool to confirm final case assessments. That is, one organization may use an SPJ process to determine the best course of action after intake—e.g., should the case be escalated to threat assessment, dismissed, or perhaps diverted to another department? Another organization may use that same tool after a threat assessment case has been completed as a way to check a professional judgment against the results of the SPJ. While these examples represent the use of tools at both the entry and exit points of a case assessment, there was no identifiable theme to these practices. Rather, it suggests that there is a range of variation in how tools are utilized at different points in the threat assessment process by different threat assessment professionals.

During our interviews, we also encountered an unexpected use of SPJ tools that, while not prominent across all interviews, is noteworthy. Specifically, in some cases use of tools is also to obtain the appropriate language to handle cases as they are referred back to the manager, or whoever asked for the assessment in the first place. This can mean providing formal language to those who are receiving the assessments to provide a sense of security and professionalism. That is, seeing the scores and language around a particularly concerning case may help alleviate some of the concerns regarding that case. In addition, it was described as providing a framework for translating threat assessment work to concerned parties in the appropriate language and with the appropriate terminology. This can also be characterized as process documentation, providing certainty to managers that the process was thorough and that the original concern isn’t being dismissed.

Training consistently came up as a top concern during our interviews. Interestingly, interview notes coded for ‘developed tool usage,’ or discussions regarding the usage of existing SPJ tools (WAVR-21, TRAP-18, etc.) in threat assessment practice also identified training as a top concern. This relationship is reflected in Figure 7. Word frequency queries also identified WAVR-21 and TRAP-18 as the most cited SPJ tools utilized by threat assessment professionals in our interviews. Stalking tools, such as the Stalking Risk Profile (SRP), were also frequently cited. The results of this query are presented as a Word Cloud in Figure 7.

**Finding 4: Variability in Tool Coverage**

Another primary theme that came up in our interviews was the application of tools to various scenarios. Many of the practitioners we interviewed were responsible for a range of threat assessment scenarios.

---

"IT'S SO CLEAR IN TERMS OF THE INTERVENTION, THE PREVENTION, AND THAT THESE ACTIVITIES, THIS STRUCTURE, THIS PROCESS WORKS, AND WE SEE IT EVERY DAY." - INTERVIEW #10
Of course, the needs of a particular threat management team will ultimately determine the range of tools best suited for that team. However, multiple practitioners expressed discontent over the range of scenarios individual tools covered. That is, most threat assessors cover at least some small range of threat assessment needs. For example, a threat assessment team for a school district may utilize WAVR-21 for assessing the risk of violence on campus, but they may also need access to ERG-22+ (examining the extremist offender risks) on occasion due to the nature of some cases (Powis et al., 2019). While WAVR-21 may be the most heavily utilized and relied upon tool, access to ERG-22+ may be more limited due to budgetary constraints, making it a potentially unrealistic choice for smaller organizations with limited resources. Cost constraints aside, practitioners also expressed concern over how realistic training in multiple tools may be, especially with limited staffing. For example, if someone has been trained on a tool one time they’ve only used twice, can their expertise on that tool be trusted?

Because of these concerns, multiple practitioners we spoke with had been involved with developing their own assessment tool tailored to their departmental needs. Generally, these tools build off the parts of existing tools that they like or that are most applicable to their needs, although one team we spoke with had received significant funding to develop their own psychometric behavioral threat assessment tool. In addition, issues regarding applicability and budgetary constraints were cited by those we spoke with who did not use any SPJs in their day-to-day operations.

**Finding 5: Program Development Challenges**

Another recurring theme by program leaders/managers was the lack of a starting point when developing threat assessment teams/departments/programs. Most of the program leaders we spoke with described a process of ‘going at it alone,’ and having to create threat assessment strategies and practices based on their own research and efforts. Managers described a self-education process, where they had to search out best practices, available tools, training, and oftentimes, funding opportunities. Other managers described advocating to leaders within their organization for the need and/or development of behavioral threat, which was the origin of their program development efforts at times.

Essentially, most of those we talked to describe figuring it out independently to develop their program—while tools exist, there’s no real ‘playbook’ on how to use them, especially for specific applications. In addition to organizational differences, this likely helps account for the range of practices in tool application. While individual departments will need to develop programs based on their unique needs, some guidelines for initial program development could be helpful, especially for smaller organizations with fewer resources and relationships with more established departments.

**Finding 6: Variability in Organizational Approaches**

Most interviewees described intentionally developing an interdisciplinary team to conduct threat assessment. The composition of these teams ranged but often included a threat assessment practitioner, a psychologist, and a legal expert of some sort, such as a trained attorney. They often stressed the importance of this interdisciplinary approach to conducting threat assessments—people are complex, and bringing in a range of expertise and approaches provides a more robust and holistic approach to the assessment process. While some teams are simply one or two individuals, making an interdisciplinary approach unrealistic, those with larger programs and more extensive resources stressed the importance of bringing in a range of experts from different fields when conducting assessments.

While an interdisciplinary team was frequently cited as the ideal, the approaches these teams took to the assessment process varied widely from one organization to the next. For example, while some
managers stressed the importance of speaking directly with the individuals being assessed, others have a no-contact policy and only speak to those around the individual. Some take a highly structured approach to threat assessment that relies heavily on tools and guidelines, whereas others take a more clinical, practitioner judgment approach, regardless of tools. Not only are tools utilized in different ways between different organizations, but the overall approach to managing threat assessment cases can vary dramatically from one organization to the next.

**Finding 7: Variability in Individual Approaches (individual beliefs)**

Individual approaches refer to content about an individual’s beliefs regarding threat assessment, including management, philosophy, and so on. This is distinct from organizational approaches in that it refers to personal beliefs and approaches to threat assessment that exist apart from their respective organizations. Many described viewing threat assessments as one tool in a toolbox against violence, with one explaining that what they want, and see as the best practice, is to have a model with a toolbox of these tools that they can utilize, or at least have access to individuals well versed in those tools. Many describe a strong personal commitment to the practice and seem to sincerely view this as the future of violence prevention in the United States.

**Finding 8: Issues and Challenges are a Part of Threat Assessment Work**

An issue that frequently came up was the problem of buy-in by those who are needed to either collect information, utilize tools, or trust in the process. This was especially prominent among those involved in law enforcement but buy-in can also be a problem for any practitioner seeking funding and authorization. That is, securing funding can rely on buy-in to behavioral threat assessment practices by those responsible for approving funds and programs.

Buy-in among law enforcement officers poses a particular challenge. Law enforcement culture is focused on arrests—however, threat assessment is a completely different approach that revolves around information gathering and then implementing interventions that bolster protective factors to *prevent the need for an arrest*. This speaks to a larger trend in law enforcement of officer buy-in of community policing (Shupard & Kearns, 2019). There can be buy-in issues at other levels as well – policymakers for instance – who are needed to approve funding. Despite this, many of our interviewees expressed a sincere passion and belief in the value of behavioral threat assessment.

The focus on risk factors over protective factors across various SPJ tools was another concern voiced by some professionals. While understanding risk factors is an important and crucial component of risk assessment, actually preventing acts of violence requires interventions and ways to bolster protective factors. This was described as an important component of taking a holistic approach to threat assessment. Some managers expressed frustration in a perceived over-emphasis on risk factors over protective factors on many SPJ tools they utilized.

“**HUMANS ARE DYNAMIC—WE NEED GOOD INFORMATION TO MAKE A GOOD ASSESSMENT.”** – INTERVIEW #7

Lastly, a frequently cited issue when using SPJ tools was the level of data required for tools. That is, SPJ tools are very data-intensive, and require significant background information to provide assessments. Given the range of issues regarding resources and buy-in, this provides another potential roadblock because it can increase the amount of time needed on each case, or result in inferior assessments due to lacking information. For example, if law enforcement officers are primarily responsible for data collection, they may dismiss the need for the level of data involved, as most SPJ tools are data heavy, and collecting data on non-offenders is generally outside of their scope and training. An officer without a foundation in threat assessment may not appreciate how crucial all components are, and as one interviewee stated succinctly, our assessments are only as good as the data
we input into them. This may be in part due to buy-in issues, but also the contrast between standard investigative policing practices. While standard policing utilizes investigations to collect data to charge cases, threat assessment requires extensive data collection with the goal of, in ideal cases, avoiding criminal sanctions altogether.

In addition, if the level of data required is inferior or not fully collected, the assessments provided by tools may be incomplete or even completely inaccurate, rendering the tool not only functionally useless but potentially counter-productive, if cases that need interventions are instead kicked out due to insufficient data. In short, an SPJ outcome is only as good as the data that is put into it.

**Findings 9a and 9b: Insider and Novel Threats**

**Insider Threats**—While some departments primarily handle insider cases (such as those involving military actors), those who handled a range of cases generally described insiders in the same terms as other types of threats—the behavioral indicators are the same, regardless of whether they are an insider. The only significant difference described with these threats was the access to information available to case managers—organizations are going to have data already available on insiders, cutting down on some of the data gathering requirements, resulting in more streamlined assessments and better access to the data required for SPJs. Generally, threat assessors are dealing with potentially violent cases, and at times non-violent insider cases (espionage for example) were referred to exterior departments.

**Figure 8. Insider Threats Word Frequency Cloud**

Further, multiple organizations described having insider threat teams that focused predominately on cybersecurity, where potential cybersecurity insider threats may be referred to more general threat assessment teams.

**Novel Threats** As part of the interview process, individuals were asked whether novel threats represented a unique challenge in threat assessment. Responses varied for this question, with some interviewees indicating that the tools are designed to be threat-agnostic and should work in most contexts. For others, there was some indication that the threat landscape is shifting and that some tools may not be as adept at capturing novel threats as others. There was also some indication that tools utilizing the SPJ approach inherently rely on the judgment of the practitioner and for novel threats, a lack of exposure to a threat (i.e., because it is novel, there has not been exposure) means it is difficult to categorize or quantify that threat. Given this variability, there remain several “unknowns” about novel threats and the utility of current threat assessment tools.

**Figure 9. Novel Threats Word Frequency Cloud**
Supplemental Findings: Sentiment analysis

Sentiment analysis uses Natural Language Processing to automatically detect and code text by sentiment across a 6-point Likert Scale, ranging from Very Negative to Very Positive.

![Sentiment by Code](image)

Figure 10. Sentiment by code across all interviews

When we consider the sentiment across our full coding scheme, we see that overall, there is a fairly equal distribution of negative vs. positive sentiment across all 13 of our interviews, with a slight trend towards negative sentiment. This is represented in Figure 10. Generally, considering the context of our interviews, negative sentiment can be interpreted as topics where our interviewees felt there was a need for improvement. Not surprisingly, “issues encountered” stands out as containing the most negative content. In addition, “training” also stands out as containing a high level of negative sentiment. Training has consistently stood out as a top theme across interviews, for a range of reasons, many revolving around needed improvements. This sentiment analysis bolsters our finding that training is a top concern among practitioners and is an important focus area for future research.

When we break down the sentiment across the training sub-codes, we see that none of the training-coded content is rated very positively. This breakdown is illustrated in Figure 11. Surprisingly, the “Other” category accounts for this trend toward negative sentiment across training content. Most of the comments in the “training—other” subcode regard comments about what has and has not worked in prior training, as well as recommendations for improving the training process. Essentially, the other category captures comments that did not fit into the training themes of Foundation, Cost, Time, and Strategy. Regarding Strategy and Time, there was not enough content to apply the sentiment analysis.
While our sample may be limited concerning generalizability, this suggests that 1) our interpretation of the interview results regarding training aligns with the findings from the sentiment analysis and 2) training remains a complex issue regarding the use of threat assessment tools and is worthy of further inquiry.

Overall, our sentiment analysis suggests that feelings regarding the state of threat assessment—at least, among our interview subjects—are generally well balanced, but that certain issues, predominately those around training, continue to stand out as a top concern.

![Sentiment by Training Codes](image-url)

**Figure 11.** Sentiment by training

**Limitations around Generalization**

Although we began to reach saturation (i.e., interview findings began to repeat and similar themes emerged) in our interview responses, it must be noted that a total interview sample of 13 obtained from snowball and convenience sampling is far from representative, and these findings should not be seen as speaking for all threat assessment professionals across all industries and sectors. Instead, these results should be seen as highlighting potential themes, issues, and real-world applications that are overlooked in the literature and in more systematic reviews. That is, these interviews provide a snapshot into the real-world use of tools and approaches to threat assessment.

**CONCLUSIONS**

Our interviews provided several noteworthy findings. In many ways, what we found aligned with the existing literature on threat assessment practices. However, the human side of threat assessment is more challenging to glean from research studies and evaluations, and our interviews provided several significant insights into the real-world application of threat assessment instruments, as well as provide a snapshot of the application of threat assessment across several domains.

Our primary conclusion is that practitioners or organizations across contexts may utilize the same threat assessment instruments at different points in the threat assessment process. In addition, different practitioners or organizations may utilize the same instruments for different purposes. For example, one practitioner may utilize the WAVR-21 for triaging purposes, to determine whether a case requires further threat assessment, whereas another manager may utilize the WAVR-21 to verify the results of their completed threat assessment. A third might then use it for of threat assessment as a standalone tool. Broadly, this suggests that 1) there is a need for assessment tools at various points in the process and 2) there may not be strong guidance on how exactly assessment tools should be utilized in the assessment process. This also speaks to the frequently referenced need for a strong foundation of training in assessment tools, as well as the need for refresher training regularly.

Interestingly, tools were also utilized for purposes outside of traditional case assessment. In one noteworthy example, a threat assessment manager informed us that they utilize tools to provide the
appropriate language to assure those making referrals, as well as provide the appropriate language and support to promote buy-in from leaders. While again, it must be noted that this is one example from a non-representative sample, and therefore does not speak for threat assessment as a whole, it does suggest that tools may be utilized in ways other than their original intent, which may be worthy of further empirical exploration down the road.

Another takeaway that occurred throughout our interviews was the challenges interviewees experienced in obtaining buy-in, be it from leaders, policymakers, colleagues, or even, the public. This was especially prominent with law enforcement, who cited challenges in receiving buy-in from both leadership and fellow officers. This finding is perhaps not surprising, given that law enforcement officers are trained to apprehend offenders, rather than prevent them from offending in the first place. However, several of our respondents suggested that, once one is trained and experienced behavioral threat assessment, one can quickly see the value. Again, while non-representative, this may speak to larger challenges with buy-in at the leadership level.

In addition, the many challenges and needs associated with training stood out as a primary conclusion across interviews. Surprisingly, cost was one component, but did not stand out as the main component of this theme. Rather, the need for strong foundational training, alongside regular practice, and refresher training, was a prominent point across interviews. In short, if a department were to only complete a handful of assessments in a calendar year, they wouldn’t retain the skills obtained in initial training, and therefore, the assessment may be lacking. And, without a strong training foundation, improper tool use may pervade an organization, resulting in inferior threat assessments and increasing risk.

Finally, a common issue among those in leadership positions was the lack of a starting point of guidelines for developing threat assessment programming. That is, managers had to “figure it out for themselves,” and piece together what was needed for a proper threat assessment program. Although different organizations will obviously have different needs, more standardization or guidelines may be beneficial in promoting threat assessment program development at various levels.

To close, through a combination of formalized analysis and qualitative consideration, the interviews revealed several key issues around threat assessment that are not readily gleaned through traditional validation metrics. These issues offer both unique and critical avenues for future investigation and we see tremendous value in future systematic investigation of end-user perceptions and use-case application.
What Works in Threat and Risk Assessment, for Whom, and in What Circumstances?
The State of the Evidence

NCITE Consortium Research Team
Paul Gill – University College London
Zoe Marchment – University College London
Amber Seaward – University College London
Introduction

The systematic review presented earlier in this report synthesized what was known about risk and threat assessment instruments, their psychometric properties, and predictive capabilities. It was noted that the human element of threat and risk assessment processes remained unsynthesized. This ‘state of the science’ briefing note acts as a first step toward such a synthesis. We argue that such factors are far more consequential for real-life harm reduction than an instrument’s predictive powers, especially so when low base rate events are the subject of inquiry.

To synthesize this evidence, we conducted another systematic review. We conducted a keyword search of titles and abstracts in Psycnet for papers published from database inception until 3rd November 2021, restricted by the English language. Key words searched for issues related to problems of interest (insider**, OR “violenc” OR “terrorist” OR “radical”** OR “crim”** OR “recidiv” OR “offen”** OR “extremis” OR “aggresssi” OR “threat” OR “arrest” OR “reoffen”** 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 judgment” OR “SPJ”), and evaluations (“evaluat”** OR “effect”** OR “outcome”** OR “program”**). Five researchers sifted through 7,259 studies and judged their title and abstract based on whether the study (a) concerned risk/threat assessment (b) was an evaluation (c) was a process evaluation (d) had some empiricism. 48 full papers made it through this initial sift. For this briefing note, 21 were excluded because they were not peer-reviewed papers but will be incorporated into future updates. Only 27 studies therefore met all of our initial criteria. To put this into context, our previously submitted literature review of the psychometric properties of risk assessment instruments covered 2,108 empirical studies. There is a huge disparity, and this reflects a real lack of focus on the human aspect of threat and risk assessment.

To organize our results to date, we utilize the EMMIE framework, developed for the UK ‘What Works Centre for Crime Reduction’ at the Department of Security and Crime Science at University College London (see http://whatworks.college.police.uk/toolkit/AbouttheCrimeReduction-Toolkit/Pages/About.aspx). EMMIE is an acronym denoting five categories of evidence relevant to policing and crime prevention (see Box 1 below). It was inspired by the ‘realist’ approach to evaluation (Pawson & Tilley, 1997), which directs evaluators to ask not only whether an intervention ‘worked’ – the dominant question in the crime prevention literature - but how an intervention worked (or not), why, for whom, and under what conditions is it more or less effective. Just as importantly, EMMIE calls attention to ways in which some interventions may inadvertently backfire under particular conditions. EMMIE was designed to help disentangle the many components of a complex intervention to generate insight into the features that support its success (or otherwise).

The EMMIE framework is especially relevant to threat and risk assessment due to its multi-method focus which combines process and outcome evaluation traditions. It offers a dynamic, holistic means of understanding how processes work. This helps to elicit working theory and tease out contextual variation, which is likely given the vast array of contexts in which threat and risk assessments play out.
Box 1. The EMMIE framework

**Effect – has it worked?**

The first ‘E’ of EMMIE refers to ‘effect’ size. Typically, this focuses on the ‘effect’ of an intervention but can also be extended to other non-traditional effects (e.g. the formulation itself, the management plan).

**Mechanism – how did it work?**

The first ‘M’ refers to the ‘mechanism’ through which an intervention brings about its effect – the ‘active ingredient’ so to speak. This is important in determining what needs to be done to produce (or avoid) a given outcome.

**Moderator – what conditions are needed for it to work?**

The second ‘M’ refers to ‘moderators’ (or ‘contexts’) – the conditions that are instrumental for an intervention to activate the mechanisms.

**Implementation – what was found to be needed to put it in place?**

The ‘I’ refers to ‘implementation’ conditions that support or obstruct the delivery of the intervention (this would include reliability testing).

**Economics – is it cost-effective?**

Finally, the second ‘E’ refers to ‘economics’ – what the intervention will cost in relation to outputs, outcomes, or benefits (Manning et al., 2016).

The following pages briefly summarize the state of the science emanating from published peer-reviewed process evaluations of threat and risk assessment procedures:

### Effects (has it worked?)

<table>
<thead>
<tr>
<th>Key Finding</th>
<th>Evaluation Method</th>
<th>Instrument / Setting</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users report risk assessment instruments as useful and valuable to everyday practice.</td>
<td>Police officer survey (n=213)</td>
<td>Range of intimate partner violence risk assessment instruments</td>
<td>Campbell et al. (2018)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=42)</td>
<td>Practitioners dealing with child sexual exploitation</td>
<td>Franklin et al. (2018)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td>Assessment outcomes strongly impact perceptions of offending likelihood but are rarely the sole criteria that factor into an opinion.</td>
<td>User survey (n=109)</td>
<td>Static99R</td>
<td>Chevalier et al. (2015)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Practitioner survey (n=42)</td>
<td>Practitioners dealing with child sexual exploitation</td>
<td>Franklin et al. (2018)</td>
<td></td>
</tr>
</tbody>
</table>

### Mechanisms (how did it work?)

<table>
<thead>
<tr>
<th>Key Finding</th>
<th>Evaluation Method</th>
<th>Instrument / Setting</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessments help prioritize key risk and protective factors that require treatment/intervention/boosting.</td>
<td>Case file analysis (n=107)</td>
<td>Case Management Strategies</td>
<td>Dhaliwal et al. (1994)</td>
</tr>
<tr>
<td></td>
<td>Case file analysis (n=216)</td>
<td>Offender Assessment System (OASys)</td>
<td>Kewley et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td>Users report risk assessments help focus minds on problems/concerns, map risk and level of risk, guide decision-making and client interviews, help with team building, provide consistency of language, and are useful to potential victims to show concerns being highlighted.</td>
<td>Practitioner survey (n=42)</td>
<td>Practitioners dealing with child sexual exploitation</td>
<td>Franklin et al. (2018)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=88)</td>
<td>WARRN, Child and adolescent mental health services</td>
<td>Gray et al. (2019)</td>
</tr>
<tr>
<td></td>
<td>Practitioner interviews (n=10)</td>
<td>Multi-Agency Risk Assessment Conferences</td>
<td>Robinson (2006)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td>Risk assessments open avenues for specific types of treatment and interventions.</td>
<td>Referrer interviews (n=31)</td>
<td>NHS Lothian Sex Offender Liaison Service</td>
<td>Judge et al. (2014)</td>
</tr>
<tr>
<td>Risk assessment can negate potential biases about certain types of victims.</td>
<td>Case file analysis (n=867)</td>
<td>B-SAFER</td>
<td>Storey &amp; Strand (2017)</td>
</tr>
<tr>
<td>Risk assessments (a) by partner agencies for police and (b) by police for partner agencies, help improve and inform decision-making, objective analysis, and case management.</td>
<td>Police officer survey (n=213)</td>
<td>Range of intimate partner violence risk assessment instruments</td>
<td>Campbell et al. (2018)</td>
</tr>
<tr>
<td></td>
<td>Referrer survey (n=14)</td>
<td>The Integrated Threat and Risk Assessment Centre</td>
<td>Ennis et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>Referrer interviews (n=31)</td>
<td>NHS Lothian Sex Offender Liaison Service</td>
<td>Judge et al. (2014)</td>
</tr>
<tr>
<td></td>
<td>Embedded observatory design</td>
<td>Multi-Agency Risk Assessment Conferences</td>
<td>Robinson (2006)</td>
</tr>
<tr>
<td>Training significantly improves the identification of (critical) risk factors, risk levels, and the quantity and quality of suggested management strategies that correspond to identified risk factors. Training also improves participants’ rationale for their decisions. Trainees reported greater levels of confidence and perceived competence in risk assessment.</td>
<td>Practitioner survey (n=96)</td>
<td>SARA, SAM, HCR20</td>
<td>Storey et al. (2011)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Training on a specific instrument significantly improved self-reported skills in formulation, risk management/safety planning, and risk communication. Training also improved self-reported confidence, service user safety, general-public safety, and ability to save lives. Training also improves information sharing and communication across agencies.</td>
<td>Practitioner survey (n=88)</td>
<td>WARRN, Child and adolescent mental health services</td>
<td>Gray et al. (2019)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=85)</td>
<td>CARDS, Clinical sites</td>
<td>Watts et al. (2004)</td>
</tr>
<tr>
<td>Threat assessment training improves the understanding of basic concepts and guidelines for conducting a threat assessment, the understanding of specific forms of violence, helps responses to threats of violence and motivates participants to use threat assessment principles in their practice.</td>
<td>Education practitioners (n=4,666)</td>
<td>Comprehensive Student Threat Assessment Guidelines</td>
<td>Stohlman et al. (2020)</td>
</tr>
<tr>
<td>Training in risk formulation significantly improves user perception of instrument effectiveness, anticipated impact upon future work, anticipated impact upon managing risk, perceptions of how easy it is to complete, and perceived relevance to clinical practice.</td>
<td>Clinician survey (n=131)</td>
<td>HCR20-v3</td>
<td>Covernton et al. (2019)</td>
</tr>
<tr>
<td>Risk assessment training increases the likelihood of a formulation and risk management plan being articulated even in the absence of a specific instrument being used.</td>
<td>Case file analysis (n=100)</td>
<td>Hospital setting</td>
<td>Sundrum &amp; Browne (2004)</td>
</tr>
<tr>
<td>Limited or inadequate resourcing negatively impacts the ability for risk management plans to be actioned.</td>
<td>Referrer survey (n=14)</td>
<td>The Integrated Threat and Risk Assessment Centre</td>
<td>Ennis et al. (2015)</td>
</tr>
</tbody>
</table>

**Moderators (what conditions are needed for it to work)?**

<table>
<thead>
<tr>
<th>Key Finding</th>
<th>Evaluation Method</th>
<th>Instrument / Setting</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thorough assessments require information from a range of sources.</td>
<td>Single case study</td>
<td>Threat assessment in schools</td>
<td>Goodrum et al. (2018)</td>
</tr>
<tr>
<td>Key Finding</td>
<td>Evaluation Method</td>
<td>Instrument / Setting</td>
<td>Citation</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Failure to do so risks an incomplete picture and harm being realized. Poor information sharing practices can negatively impact the success of threat assessment. Issues regarding confidentiality are a consistent concern.</td>
<td>Practitioner interviews (n=10)</td>
<td>MultiAgency Risk Assessment Conferences</td>
<td>Robinson (2006)</td>
</tr>
<tr>
<td>The inability to consider alternative scenarios in changing and complex environments can negatively impact threat assessments.</td>
<td>Single case study</td>
<td>Government cybersecurity department</td>
<td>Ceric &amp; Holland (2019)</td>
</tr>
<tr>
<td>Older and more experienced respondents report higher perceived usefulness for risk assessment instruments.</td>
<td>Police officers (n=213)</td>
<td>Range of intimate partner violence risk assessment instruments</td>
<td>Campbell et al. (2018)</td>
</tr>
<tr>
<td>High staff turnover and poor knowledge of existing resources negatively impact multi-agency working.</td>
<td>Referrer survey (n=14)</td>
<td>The Integrated Threat and Risk Assessment Centre</td>
<td>Ennis et al. (2015)</td>
</tr>
<tr>
<td>Different professional backgrounds benefit equally from training.</td>
<td>Education practitioners (n=4,666)</td>
<td>Comprehensive Student Threat Assessment Guidelines</td>
<td>Stohlman et al. (2020)</td>
</tr>
<tr>
<td>Refresher workshops significantly increase adherence to guidance protocols.</td>
<td>5 users coding 60+ cases each</td>
<td>START:AV</td>
<td>De Beuf et al. (2020)</td>
</tr>
<tr>
<td>Slow assessments lead to negative perceptions from referrers.</td>
<td>Referrer survey (n=14)</td>
<td>The Integrated Threat and Risk Assessment Centre</td>
<td>Ennis et al. (2015)</td>
</tr>
<tr>
<td>Without standardized training, users of the same instrument who have different professional backgrounds are likely to (a) use the instrument differently and (b) interpret a single instrument’s risk scores differently.</td>
<td>User survey (n=95)</td>
<td>Psychopathy Checklist Revised</td>
<td>Boccaccini et al. (2017)</td>
</tr>
<tr>
<td></td>
<td>User survey (n=109)</td>
<td>Statio.99R</td>
<td>Chevalier et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>Case file analysis (n=72)</td>
<td>Statio.99R, MnSOST-R</td>
<td>Murrie et al. (2009)</td>
</tr>
<tr>
<td></td>
<td>Case file analysis (n=398)</td>
<td>Psychopathy Checklist Revised</td>
<td>Murrie et al. (2012)</td>
</tr>
<tr>
<td>Different trainers, providing the same training materials, can have significantly different impacts on how much participants learn.</td>
<td>Education practitioners (n=4,666)</td>
<td>Comprehensive Student Threat Assessment Guidelines</td>
<td>Stohlman et al. (2020)</td>
</tr>
</tbody>
</table>

**Implementation (what was needed to be put in place?)**

<table>
<thead>
<tr>
<th>Key Finding</th>
<th>Evaluation Method</th>
<th>Instrument / Setting</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Risk assessment matters, but only when implemented well.”</td>
<td>Multi-site process and</td>
<td>Youth Level of Service/Case</td>
<td>Vincent et al. (2016)</td>
</tr>
<tr>
<td></td>
<td>outcome evaluation</td>
<td>Management Inventory; SAVRY</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Users often do not adhere to the guidance in a variety of ways including reporting risk, coding, and document keeping. Quality assurance, refresher workshops, and supervisory input is therefore needed.</td>
<td>User survey (n=95)</td>
<td>Psychopathy Checklist Revised</td>
<td>Boccaccini et al. (2017)</td>
</tr>
<tr>
<td></td>
<td>User survey (n=109)</td>
<td>Static99R</td>
<td>Chevalier et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>Field study</td>
<td>START:AV</td>
<td>De Beuf et al. (2020)</td>
</tr>
<tr>
<td></td>
<td>Case file analysis (n=34)</td>
<td>HCR20v2</td>
<td>Gough et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>User survey (n=95)</td>
<td>Psychopathy Checklist Revised</td>
<td>Boccaccini et al. (2017)</td>
</tr>
<tr>
<td>Practitioners might push back against risk assessment instruments that do not provide for professional discretion in decision-making. It is important to provide users with some discretion and avoid a ‘tick box’ culture.</td>
<td>Police officer survey (n=213)</td>
<td>Range of intimate partner violence risk assessment instruments</td>
<td>Campbell et al. (2018)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=42)</td>
<td>Practitioners dealing with child sexual exploitation</td>
<td>Franklin et al. (2018)</td>
</tr>
<tr>
<td>Training parameters and content need to be signposted in advance.</td>
<td>Practitioner survey (n=27)</td>
<td>HCR-20v1</td>
<td>Garrett &amp; Rowe (2004)</td>
</tr>
<tr>
<td>Understanding user needs is essential for continued upskilling.</td>
<td>Practitioner survey (n=88)</td>
<td>WARRN, Child and adolescent mental health services</td>
<td>Gray et al. (2019)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td>Users report documentation and processes can take too long and/or are resource-intensive. Systems need to be put in place to reduce this burden.</td>
<td>Practitioner survey (n=88)</td>
<td>WARRN, Child and adolescent mental health services</td>
<td>Gray et al. (2019)</td>
</tr>
<tr>
<td></td>
<td>Referrer interviews (n=31)</td>
<td>NHS Lothian Sex Offender Liaison Service</td>
<td>Judge et al. (2014)</td>
</tr>
<tr>
<td></td>
<td>Practitioner interviews (n=10)</td>
<td>Multi-Agency Risk Assessment Conferences</td>
<td>Robinson (2006)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=28)</td>
<td>START:AV</td>
<td>Sher &amp; Gralton (2014)</td>
</tr>
<tr>
<td></td>
<td>Practitioner survey (n=85)</td>
<td>CARDS, Clinical sites</td>
<td>Watts et al. (2004)</td>
</tr>
</tbody>
</table>
### Economics (is it cost-effective?)

<table>
<thead>
<tr>
<th>Key Finding</th>
<th>Evaluation Method</th>
<th>Instrument / Setting</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic training programs for risk assessment are equally as effective as faceto-face programs as measured by performance in a post-training skill acquisition test. However, the estimated per-trainee cost of electronic training was one-third of the cost.</td>
<td>Practitioner survey (n=87)</td>
<td>Ontario Domestic Assault Risk Assessment</td>
<td>Hilton &amp; Ham (2015)</td>
</tr>
<tr>
<td>Risk assessments lead to a more appropriate allocation of intervention resources that are matched to risk level.</td>
<td>Case file analysis (n=464)</td>
<td>Structured Assessment of Violence Risk in Youth (SAVRY)</td>
<td>Vincent et al. (2012)</td>
</tr>
</tbody>
</table>
Supplemental Reports: Blind Spots in Threat & Risk Assessment

The primary focus of this report was on synthesizing and summarizing the state of science around measurement issues surrounding threat and risk assessment. To do so, we presented the state of the science review on current tools and validation evidence. In addition, we interviewed a number of practitioners who use these tools, asking what common use cases are and whether there is consistency in application. These interview findings revealed notable variability in use cases, highlighting the need to consider additional issues in threat assessment that may not emerge from a simple overview of validation evidence. To that end, we generated four additional reports tied to identifying and mitigating potential blind spots in threat assessment. The first was a potential blind spot tied to a domestic focus of threat assessment. To mitigate this blind spot, we turned to our international colleagues for guidance on lessons learned from our international partners engaging in threat assessment. The second was a potential blind spot emerging from a fixation on federal cases of threat assessment. To mitigate this blind spot, we turned to lessons learned from state and local law enforcement. The third blind spot we considered was one around the issue of a long-standing focus on external threats when there is increasing evidence around the importance of also considering insider threats. As such, we discuss emerging and key issues around insider threats. Finally, we identified a potential blind spot around novel threats, where new or emerging threats can be dismissed simply due to their novelty. We offer strategies for mitigating biases around novel threats. Each of these blind spots and lessons learned are discussed in the following sections.
Blind Spot A: Removing Domestic Fixation by Turning to Lessons from Our International Partners

The first blind spot explored involves removing fixation on domestic approaches to threat and risk assessment. To accomplish this, two reports, led by the research team at UCL, examine what threat assessment models are currently being utilized around the world and how they may differ from those used in the United States.
What Works in Threat and Risk Assessment, for Whom, and in What Circumstances?
The State of the Evidence ii

NCITE Consortium Research Team
Amber Seaward – University College London
Zoe Marchment – University College London
Paul Gill – University College London
A Directory of Threat Assessment Models

Executive Summary

- 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 behaviors (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 & Vossekui, 1997) and Safe School Initiative (Vossekui et al., 2004). These two studies analyzed the personal histories and pre-incident behaviors 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 & Vossekui, 1997; Vossekui 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 & Vossekui, 1997; Vossekui 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 behavior (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 standardized 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 behaviors 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 behavior 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 offense, and those outside the profile might be missed (Reddy et al., 2001). Therefore, threat assessment examines the escalation of behavior over time and corroborates information from multiple sources to reach a level of concern (Reddy et al., 2001; Vossekui et al., 2015).

Finally, threat assessment differs from the traditional operations of law enforcement in investigating threats after a violent offense 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 standardized 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 analyzed 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:**
a 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 well-being, 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 recognized 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 studies¹. Five researchers excluded any studies that did not concern relevant problem

---

¹ We conducted a keyword search of titles and abstracts in PsychNet 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 terrori* OR radical* OR crim* OR recidiv* OR offen* OR extremin* OR aggressi* OR threat* OR arrest* OR reoffen* OR reoffen* 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
behaviors 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.

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 phrases² 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 program (Gill & Marchment, 2020) was selected for inclusion.

**Included Studies**
The 48 included studies described 27 existing threat assessment models. These are categorized 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 "fixed").
<table>
<thead>
<tr>
<th>Schools</th>
<th>USA</th>
<th>Europe</th>
<th>Australia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Guidelines</td>
<td>Cornell (2013)</td>
<td>(Germany)</td>
<td>Leuschner et al. (2011)</td>
</tr>
<tr>
<td></td>
<td>Cornell (2020a)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell (2020b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell &amp; Burnette (2021)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell &amp; Heilbrun (2016)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell &amp; Maeng (2017)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell &amp; Warren (2024)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cornell &amp; Williams (2011)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Van Dyke et al. (2004)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Van Dyke &amp; Schroeder (2006)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rappaport model</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salem Keizer/Cascade model</td>
<td></td>
<td>Van Dreal &amp; Okada (2021)</td>
<td></td>
</tr>
<tr>
<td>Universities</td>
<td>Behavioral Intervention Team at Ozarks</td>
<td></td>
<td>Mrad et al. (2015)</td>
</tr>
<tr>
<td></td>
<td>Technical Community College</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workplace violence</td>
<td>Threat Assessment Team in a large Midwestern university</td>
<td>Scalora &amp; Racionero (2021)</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coast Guard Investigative Service Threat Management Unit</td>
<td>Rutz (2021)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employee Assistance Program</td>
<td>Holbrook et al. (2019)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hughes Fullerton Critical Incident Team</td>
<td>Root &amp; Ziska (1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Navy Criminal Investigative Service Threat Management Unit</td>
<td>Van Horn (2013)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Assessment Team at Johns Hopkins University</td>
<td>Heitt &amp; Tamburo (2005)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>United States Postal Service Employee Assistance Program</td>
<td>Kurutz et al. (1996)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Queensland Fixated Threat Assessment Center and other Australian units</td>
<td>Pathé et al. (2018) Wilson et al. (2021)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>United States Capitol Police Threat Assessment Section</td>
<td>Scalora et al. (2008)</td>
<td></td>
</tr>
<tr>
<td>Violent extremism</td>
<td>Community Connect</td>
<td>Ellis et al. (2022)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Channel programme and Vulnerability Assessment</td>
<td>Gill &amp; Marchment (2020)</td>
<td></td>
</tr>
<tr>
<td>Framework (United Kingdom)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gibson (2023)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dutch National Police investigative psychologists (Netherlands)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bootsma &amp; Harbers (2021)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mixed threat forms and problem behaviors (e.g. stalking, threats, general violence, targeted violence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBI Behavioral Analysis Unit model for analysing anonymous threatening communications</td>
</tr>
<tr>
<td>Simons &amp; Tunkel (2013) Simons &amp; Tunkel (2021)</td>
</tr>
<tr>
<td>Guldimann et al. (2016)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework (United Kingdom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gudeman &amp; James (2011)</td>
</tr>
<tr>
<td>McEwan &amp; DarJee (2021)</td>
</tr>
<tr>
<td>McEwan et al. (2013)</td>
</tr>
<tr>
<td>Warren et al. (2005)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework (United Kingdom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Van Dreal &amp; Okada (2021)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Framework (United Kingdom)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maxey (2002)</td>
</tr>
</tbody>
</table>
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 behavior, even if this behavior 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 behavior (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
Standardized 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 behavior (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 recognizing 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 behavior 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.


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 standardized 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
recognized 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 setup

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 behavioral management plans, violence prevention programs, counselling, removal to on or off campus Alternative Education Programs, or referral to Youth and Family Centers for psychiatric, mediol, 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 behavior, 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 standardized 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 centers, 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 centers around the role of mental health clinicians to assess threats and build rapport, for a cohesive dynamic and to mobilize 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 mobilize 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 behavior can encompass swearing at teachers, property destruction, fighting, assaulting staff, inappropriate sexual behavior, 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 behavior 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, individualized 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 center around building rapport, explaining limits of confidentiality, assessing context and safety. For family and school staff, they center 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, behavioral 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 focusing on relieving the circumstances (both situational factors and risk factors) that worsen the risk of future violence. The model focuses 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, behaviors, 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 counselor 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 specialized assessment, targeted violence risk factors, intervention possibilities, criminal behavior expertise and attack related behaviors. 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, behavioral 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 centralized 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 Behavior 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 behaviors 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 behaviors (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 behavior 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 behaviors, 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 offense 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 behavior, which can be threats (verbal, gestural, or violent incidents) or other behaviors (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 behavior reports to staff who, if they cannot explain the behavior by the context, reports to the Prevention Appointee (Fiedler et al., 2019).

CONTACT WITH REFERRING BODIES
NETWASS centers 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 behaviors (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 behavior 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 behavior 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 following 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 behaviors. It is a flexible model, that considers behavior rather than profiling.

THREAT
Troubling behaviors 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 centers 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 to high turnover, continuously educating stakeholders in reporting procedures, and ethical issues in the frequent indirect assessment of behavior 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 behavioral analysis program aimed to facilitate intervening in concerning behavior before violence occurs. The TMU is a specialized 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 specialized 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, centralized, and specialized 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 behaviors 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. \textit{Referal} CGIS receives a report and refers this to the TMU.
2. \textit{Screening} The TMU provides initial advice and looks for any concerning or warning behaviors. The case then goes to either consult & triage or comprehensive violence threat assessment.
3. \textit{Consult} \& \textit{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. \textit{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 analyzed. 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. \textit{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 utilize 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 behavior and decide next steps, but these can be resisted when a case is old; the TMU can therefore conduct independent checkins 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 behavioral health.
- Security personnel

Referrals structure
CASE GENERATION
Employees who have been threatened or witnessed threatening behavior 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
Crossfunctional: 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 recognized 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 recognize 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 behaviors. 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 behavioral risk assessment, where the focus is not on profiling violent people, but situations where a person might exhibit violent behavior (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 counterintelligence investigations due to similarities in warning behaviors.

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 behaviors, mitigation strategies, interview questions, and case development. This setup 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 Center (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 behavior. 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 analyzed as high priority and constantly monitored and re-assessed.

RESOURCES USED IN THREAT ASSESSMENT

Various categories of resources are analyzed:

- Precise details of the wording and delivery method of the threat or concerning behavior
- 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 behavior 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 finalized 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 center 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 standardized 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 behavioral 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 followup 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 decentralized 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 behaviors, 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 standardized 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 RA Team.

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 RA Team to monitoring outcomes.

Quality/standards assurance
PERFORMANCE AND EFFICACY EVALUATIONS
The RA Team 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 RA Team 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 specialized 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 offense. 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 behaviors, 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 cohosts 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 formalize 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 roleplay 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 analyzed the concerning behavior, 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 analyze available information and conduct interviews to clarify what mental health factors are relevant, review previous evaluations, develop hypotheses about likelihood for concerning behavior 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 uses 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 behavior 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 behavior, the individual’s background, and contextual factors. These factors overall are categorised into contextual, subject, motivational, target, protective, and contact behavior.

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 reevaluation of their risk factors for predictive validity to ensure they are empirically supported. There is also analysis of patterns in concerning behaviors 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 Center**

**Summary**
The Fixated Threat Assessment Center (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 behaviors were driven by a treatable mental illness, and individuals exhibited pre-attack warning behaviors 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 behaviors (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.
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 inhouse 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 followup. (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 fixedated individuals (MacKenzie & James, 2011).

**Case management structure**
FTAC does provide followup, 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 standardized 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 centers 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 fixed 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 fixed 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 fixed 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 fixed 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 report suspicious behavior, travel, or social media activity (Pathé et al., 2018). Cases are then triaged by the TriAgency 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 fixed 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 fixed 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).

   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 behavior 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 readministered if there is a change in circumstance, or just before the case is closed to QFTAC.

5. Low concern: case is not taken on by QFTAC but they may give advice for monitoring back to the referrer (Wilson et al., 2021).

6. Medium or high concern: requires a management plan. High concern cases require an urgent response.

7. **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 behavior, 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 behavior (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 behavioral 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 behaviors. 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 behaviors 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 radicalized 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.
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 health 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 recognized 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 specialization, 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.
4. Construction of a behavioral timeline: this is a life-long timeline of observable behaviors and known facts, not judgements. These include life events, behavioral development, personality traits, social networks, actions and reactions, warning behaviors, 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 behavioral timeline and engage in a meeting, chaired by the investigative psychologists.


7. Risk formulation: a causal explanation and theory of the concerning behavior. 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 behavior 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-centered. 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 behavioral timeline to look at the relevance of risk indicators in relation to each other, focus on those especially relevant to violent extremism, proximal warning behaviors, 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 behaviors 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 behavioral 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 Behaviors (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 referer.

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 analyzes 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 preattack behavior 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 reevaluation.

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.
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 behaviors, 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, behaviors 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 behaviors. 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 (Guldemann 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 offense 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 behaviors (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 behavior, 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 behaviors 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 behavior 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 behaviors, change in behavior 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 behavior, 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 offense 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 behaviors 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 behavior, 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 behaviors and facilitate forensic mental health treatment before they become serious offenses (McEwan & Darjee, 2021; McEwan et al., 2013).

THREAT
Problem behaviors 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 offenses, 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 behaviors with or without mental illness presence, including stalking, threatening, and sex offenses (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 Center for Forensic Behavioral 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 centralized 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.
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 behavior 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 behavior, 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).


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 behavior 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 behavior, and risk judgements about persistence and harm for certain behaviors (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 sixmonthly 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).
Threat Assessment Models: Lessons From Abroad

NCITE Consortium Research Team
Amber Seaward - University College London
Zoe Marchment - University College London
Paul Gill - University College London
Project Overview

Threat assessment is a process of identifying, assessing, and managing threats of targeted violence prompted by warning behaviors (Harris & Lurigio, 2012; Meloy et al., 2021). The practice emerged in the late 1990s as a measure used by the United States Secret Service to prevent assassinations (Borum et al., 1999; Fein & Vossekul, 1999), and continued to grow and expand in the following decades. This practice began to spread to our partners abroad, with threat assessment practices and models emerging outside of the U.S. Non-U.S. models adopted and built upon the United States Secret Service model, and together the U.S. and its partners have developed several common practices in threat assessment, including: 1. A focus on prevention over prediction 2. Research-informed practice 3. Taking a public health approach 4. Multidisciplinary teams 5. The use of structured professional judgment 6. Forming a network of support services 7. Case management and monitoring 8. Training both the assessment team and referring bodies/stakeholders This report outlines the conclusion of a comprehensive review of threat assessment models in the United States and among our partners abroad, namely in Europe, the U.K., and Australia. The goal of this report is to better understand practices outside of the U.S., as well as determine what lessons from abroad may apply to the U.S. context. This research looks comparatively at U.S. (n=15) and non-U.S. (n=7) models where rich descriptive case studies were found within the scientific literature, resulting in a comprehensive review of 22 models in total. These cover a range of harms within educational settings, violent extremism, and stalking. There is significant variation within U.S. models, and generally more that unites than divides the approaches of the U.S. and our partners. Direct comparisons to the U.S. are also difficult due to an overall lack of outcome evaluations. However, researchers were able to identify some key differences between U.S. models and those abroad.

Four Lessons from Allies Abroad

Language Use
Language/tone used contains less emphasis on “threat/threat assessment,” especially in non-police settings. For example, many programs outside the U.S. avoid explicitly labeling teams as threat assessment units and use language of crisis and support to intentionally avoid stigmatization.

Widened Assessment Lens
Some models abroad look beyond explicit threats and threatening behaviors as the sole prompt for assessment and instead include other concerning behaviors such as fixation on weapons. In general, these models take a more holistic assessment of the individual and their behaviors.

Proactive Lead Generation
For many U.S. models, a referral begins the threat assessment process. In some non-U.S. models, there is a more proactive approach taken to lead generation.

Team Structure
Given threat assessment's dependence on statutory partners for referrals, building direct human connections between referring sites and the assessment agencies is important to maintain efficiency and trust in the system.

Multidisciplinary teams are common among models inside and outside the U.S. However, models from abroad often take a more deliberate approach to structuring the units to ensure multidisciplinary collaboration occurs in day-to-day practice.
**Blind Spot B: Reducing Fixation on Federal Approaches to Threat Assessment by Turning to Lessons from State and Local Law Enforcement**

The second blind spot explored involves removing a fixation on the federal level. To do this, state and local officials who participate in threat assessment techniques were interviewed and surveyed to provide a connection between the federal, state, and local levels for information sharing on best practices and potentially services and resources needed to be successful.
Lessons from State and Local Law Enforcement:
Threat Assessment Team Focus Groups & Survey

NCITE Center Research Team
Erin Kearns – University of Nebraska at Omaha
Kat Parsons – University of Nebraska at Omaha
Sydney Reichin – University of Nebraska at Omaha
Kelsey Ciagala – University of Nebraska at Omaha
Executive Summary

The National Counterterrorism Innovation, Technology, and Education (NCITE) Center at the University of Nebraska Omaha is currently leading a task to examine best practices in current threat assessment and threat management programs. The primary focus of the current document is to update NCITE’s work around lessons learned from local and state law enforcement involved in threat assessment teams along with members of those teams. Focus groups with threat assessment teams were conducted to help us gain a deeper understanding of the practices for threat assessment used at the local level, especially at the local law enforcement level.

We conducted our focus groups with threat assessment team members in communities from across the United States. Some of the communities served are state-wide, while others include mid-sized cities or rural towns. We aimed to explore both the similarities and differences in practices and challenges faced across these heterogeneous threat assessment teams.

In addition to focus groups, we conducted a targeted online survey regarding law enforcement threat assessment practices, capturing a snapshot of law enforcement practices across the nation.

The objectives of this analysis are to:

- Identify promising practices from the local level as they might apply at the federal level (and vice versa).
- To facilitate greater communication between federal and local level authorities by observing potential inroads for connection with such communities.

The first major finding highlights the importance of collaboration across organizations as well as within them. This was especially prescient for the collaboration between law enforcement and non-law enforcement members of threat assessment teams. We also find that integrating the community for both buy-in and reporting are important components of localized threat assessment. Finally, we find many of the same pain points identified in a previous analysis of 13 threat assessment practitioner interviews, which were primarily at the federal level. That is, buy-in, resources, and time are frequent barriers to effective threat assessment for both local and federal threat assessment actors (NCITE, 2023).

Introduction

The primary focus of the current document is to update NCITE’s work around lessons learned from local and state law enforcement involved in threat assessment teams along with members of those teams. We conducted focus groups with threat assessment teams around the country who serve communities that range in size but all of whom are integrally involved in threat assessment.

Sample and Procedure

Between August 2022 and February 2023, we conducted 16 focus groups with a total of 65 members of threat assessment teams around the country. We began with a local partner with whom we have a previous relationship. From there, we recruited other focus group participants through a mix of “snowball” sampling efforts and cold emailing. Of the 65 focus group participants, the plurality (n=26, 40.0%) work in an educational setting in some capacity (though school resource officers (SROs) are members of law enforcement, they are included in this category since they spend most of their workday in an educational setting), followed by law enforcement (n=17, 26.2%), and mental health professionals (n=12, 18.5%). A smaller percent of focus group participants work in a correctional setting (n=4, 6.2%) or in a position that does not fall within any of the above nor does it appear in any of the other teams.
(n=6, 9.2%). Participant information and identifiers have been masked for privacy reasons, though each focus group participant has a public-facing role as part of their day-to-day work on a threat assessment team.

We conducted our focus groups with threat assessment team members in communities from across the United States. Some of the communities served are statewide, while others include mid-sized cities or rural towns. We aimed to explore both the similarities and differences in practices and challenges faced across these heterogeneous threat assessment teams.

Focus group questions were semi-structured and open-ended, including the following topics:

- Professional backgrounds
- Threat assessment experience
- Perceptions of what works well with their current system to manage threats
- What system do you currently use to take the public’s reports on threats?
- What do you think works well with this system?
- What do you think is the most efficient part of your current system?
- What was most helpful in training on your current system?
- Perceptions of disconnects, barriers, or pain points with their current system to manage threats
- What information is usually missing in reports you receive from the public?
- Where do breakdowns tend to occur in the system you use?
- Suggestions for how to improve the system
- How could a system to manage threats be improved?
- What changes are most important?
- What would you like to see in your ideal threat assessment software system?

Focus groups were not recorded both for privacy reasons and to encourage candid discussion. Instead, focus groups were led by the Co-PI for Pillar 2 who is a senior researcher from NCITE with a PhD student GA as a contemporaneous note taker. When feasible, focus groups were conducted in-person though this was often not the case so most focus groups were conducted over Zoom. Each focus group lasted about one hour.

**Methods**

**Focus Groups Notes**

Although focus groups were not recorded, extensive contemporaneous notes were taken during each session. These notes, alongside observations by the researchers who conducted the focus groups, provided the basis for this assessment.

Finally, the focus group notes were compiled in qualitative analysis software, with each focus group serving as a unique case. The software used – NVivo – is designed for the qualitative and mixed-methods analysis of unstructured text, such as that from interviews, video, and other sources (*Using NVIVO in Qualitative Research, 2020*).

**Analysis**

For the analysis of these data, we conducted reflexive thematic analysis. Reflexive thematic analysis is an iterative qualitative process that is best geared toward understanding themes and stories that occur over a range of data points to gain a holistic understanding of the topic and speak to the guiding
research question or questions (Braun & Clarke, 2019). In this study, we use both inductive and deductive coding to identify themes across the texts that speak to the larger research question.

In this study, we use deductive coding across the focus group contemporaneous notes to identify themes across the texts that speak to the larger research question. However, because we were most interested in findings related to law enforcement, we included two a priori themes: LEO (Law Enforcement Officer) and SRO (Student Resource Officer). The remaining themes were those that emerged during the coding process.

The coding process followed the format of reflexive thematic analysis, which progressed as follows:

- **Familiarize ourselves with the data.** This stage involved simply reading through each text, and then rereading the texts while making notes on initial insights and themes.
- **Coded the data.** In this phase, we went through each text and applied my a priori codes to the content. In addition, as we coded a priori themes across the texts, we began developing my emerging codes based on my initial notes and themes that emerged while conducting the iterative coding process. After we completed an initial sweep of the data, we collated my emerging themes and completed a final coding of the data based on both my a priori and emerging themes.
- **Generated initial themes.** Upon review of my compiled and coded data, we reviewed codes across the content to develop initial themes. At this stage, we pulled codes from the a priori codes that did not speak to themes across the data. This process was repeated on the emerging codes as well. The remaining codes each represent a unique theme found throughout the texts.
- **Developed and reviewed the themes.** In this stage, we reviewed the themes for both overlap and relevance to the research question.
- **Refining, defining, and naming themes.** At this stage, we reviewed each theme and the related content independently. Theme names were refined to capture the nature of each theme. Each theme was reviewed and analyzed independently to determine the scope and focus of each theme. Next, we analyzed the overlap between themes.

The results of this coding scheme, the definition and scope of each theme, and analysis of the theme follow in the remainder of this paper. The final themes from the manual coding, the total number of references across texts, and the number of texts the themes appear in are listed below in Table 1.

**Table 2. Manually Coded Themes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Files</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trends</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Insider Threats</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>SPJ</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>SRO</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>Money</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Community</td>
<td>8</td>
<td>23</td>
</tr>
<tr>
<td>Process</td>
<td>11</td>
<td>51</td>
</tr>
<tr>
<td>Collaboration</td>
<td>11</td>
<td>67</td>
</tr>
<tr>
<td>Barriers</td>
<td>12</td>
<td>81</td>
</tr>
</tbody>
</table>
A description of each theme is listed below in Table 2.

**Table 2.** Manual Themes and their descriptions.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trends</td>
<td>Discussions of current trends in both threats and threat assessment practices.</td>
</tr>
<tr>
<td>Insider Threats</td>
<td>Discussions regarding insider threats.</td>
</tr>
<tr>
<td>SPJ</td>
<td>Discussions of Structured Professional Judgment (SPJ) tools usage (or lack thereof) by teams.</td>
</tr>
<tr>
<td>SRO</td>
<td>Discussions involving Student Resource Officers—that is, police officers who are posted within K-12 schools.</td>
</tr>
<tr>
<td>Money</td>
<td>Discussions of funding, including background, opportunities, and barriers.</td>
</tr>
<tr>
<td>Community</td>
<td>Discussion of community involvement; that is, the role of the community in the threat assessment process beyond those who are professionally involved.</td>
</tr>
<tr>
<td>Process</td>
<td>Discussion of a given team’s threat assessment procedures, practices, and process (i.e., How are cases triaged? How do teams handle cases/reports?)</td>
</tr>
<tr>
<td>Collaboration</td>
<td>Discussions of collaboration between organizations or entities for threat assessment—this can be between departments within an organization, or between two separate organizations with shared goals—such as the collaboration between a school’s threat assessment team and the local police.</td>
</tr>
<tr>
<td>Barriers</td>
<td>Discussions of barriers to threat assessment—this covers a range of pain points practitioners raised as barriers to their threat assessment practices and goals.</td>
</tr>
<tr>
<td>LEO</td>
<td>Any discussions surrounding the role of police and law enforcement officers in the threat assessment process.</td>
</tr>
<tr>
<td>Starting Point</td>
<td>Discussions of the origin and background of team members and the development of their threat assessment teams.</td>
</tr>
</tbody>
</table>

In addition to reflexive thematic analysis, we conducted automated thematic coding using a Machine Learning process that uses Natural Language Processing (NLP) to automatically detect and code broad themes across texts. This NLP tool is a function of the NVivo software package, and there are some important limitations to keep in mind when analyzing automated coding of any sort. NLP cannot understand coded language or appreciate the context of a particular sentence of a paragraph within a document. Further, like most text analysis tools, NVivo cannot recognize:
sarcasm  
double negatives  
slang  
dialect variations  
idioms  
ambiguity  

(Automatically Detect and Code Themes, n.d.)

However, when used alongside manual coding, NVivo can help 1.) serve as a check on the manual coding process by identifying similarities and 2.) highlight any potential themes that may have been missed in the manual coding process, or simply were not considered in the original research question but that still provide useful insights overall. In addition, because we are using contemporaneous notes rather than transcripts, sarcasm, slang, and similar casual language are less likely than in traditional spoken conversation.

The results of the NLP autcoded themes are outlined below, with “stop words” (i.e., those that are used frequently in the notetaking process but that are irrelevant to the content) removed, as was language including “threat” such as “threat assessment” and “threat assessment team,” as these were the main subject of the focus groups. The remaining autcoded themes are outlined in Table 3 below.

Table 3. Autocoded Themes

<table>
<thead>
<tr>
<th>Name</th>
<th>Files</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td>10</td>
<td>29</td>
</tr>
<tr>
<td>Community</td>
<td>9</td>
<td>25</td>
</tr>
<tr>
<td>Health</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>Training</td>
<td>10</td>
<td>22</td>
</tr>
<tr>
<td>Safety</td>
<td>7</td>
<td>20</td>
</tr>
<tr>
<td>Police</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>Work</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>System</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>Public</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Situation</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>Issues</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>Plan</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>Resources</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>

The remainder of this report will break down our primary findings from this analysis and their relevance to the Department of Homeland Security and its stakeholders. This includes both our most salient themes (i.e., those that appeared the most frequently across the highest number of texts) and those with the greatest relevance to the objectives stated prior.
Findings and Analysis

Finding 1: Collaboration is Key

Unsurprisingly, most of our threat assessment teams outlined the importance of collaboration across partners for an effective process. The most crucial component of this theme is collaboration with local police in any given jurisdiction. That is, regardless of team size, setting, or location, the level of collaboration with local police was frequently cited as crucial to their team’s success. However, this also involves collaboration with the community, especially on the information gathering and reporting side. As one participant noted, their cases are as good as the information they receive—if reporting is insufficient, or even overlooked, a threat assessment team has nowhere to start. Therefore, we looked at the intersection of collaboration, police, and the community.

However, this also exhibited a pain point—that is, while threat assessors rely on the information—both in the form of tips or reports and in information sharing for assessment purposes—provided by the community, community members are often unfamiliar with what is worthy of being reported or how to categorize information properly. Indeed, here we find the role of the police both crucial but also a potential pain point—that is, while threat assessment teams rely on collaboration with the police and regularly have a police officer (or school resource officer - SRO) on the team, policing culture is markedly different from those in other professional settings, especially school settings which generally involve minors. Teams that cite the most success have been able to adapt to policing culture. The key component of the success of this collaboration depends on the ability of both parties to adapt to the culture of the other, which is an intentional and mindful process.

One example of this integration is demonstrated by the comments from a focus group on a team in the K-12 system. They explained that at first, integrating with the police was difficult, largely due to these cultural barriers. However, they found a middle ground that resulted in safer school settings overall—for instance, while regular police cruisers at elementary schools were seen as scary by children, among high school students, this police presence has shown to be more beneficial.

Generally, finding the best working rhythm of collaboration between police and threat assessment teams was a process, where both sides must be mindful of the culture and rules structuring each other’s background and professional setting, and be willing to compromise as well as identify ownership for specific tasks. This finding aligns with the results from our interviews conducted with threat assessment professionals. That is, law enforcement culture is focused on arrests—however, threat assessment is a completely different approach that revolves around information gathering and then implementing interventions that bolster protective factors to prevent the need for an arrest. This speaks to a larger trend in law enforcement of officer buy-in of community policing (Shupard & Kearns, 2019).

In short, while collaboration is key, and integrating police directly, or even indirectly, into threat assessment practices is crucial, to do so can be particularly challenging due to differences in both the purpose of police vs. threat assessors, as well as significant cultural differences. As one focus group participant noted, it is a matter of finding the right people. That is, someone who is open-minded and willing to work with threat assessors rather than around them.

Finding 2: Community matters a great deal

As noted in the previous section, the integration of the community into threat assessment practices is another crucial component of best practices overall. However, the role of the community in shaping local threat assessment practices extends beyond its role in collaborating with threat assessors and police. That is, one of the pain points regularly cited was a lack of awareness by the general community. In
addition, community buy-in was raised as a pain point, with smaller community members often sharing a sentiment of “that stuff doesn’t happen here.” Therefore, even with strong reporting avenues and community awareness, community buy-in is another important component of successful collaboration with threat assessment officials.

With that said, there are some promising practices identified that seem to facilitate and engage the surrounding community in the threat assessment process. That is, successful teams saw not only collaboration between local police and organizations but also, that police who maintained a presence and relationship with community members had better rates of reporting and higher quality information gathering. This aligns with community policing best practices, which contend that police contact with the community should occur outside of arrests and other negative interactions and that instead, police should be engaged and integrated into the communities in which they operate (Schanzer et al., n.d.; Shupard & Kearns, 2019).

**Finding 3: Current events prompt progress**

Most of the threat assessment teams we spoke with cited a particular tragedy that was the antecedent to either the development of a threat assessment team or process or of improvements or refinements to existing threat assessment efforts. Sandy Hook was cited by several as their motivating force, and several noted that they doubted their efforts would have been as successful nor as expedient if it were not for the dramatic nationwide tragedy that preempted them. On multiple occasions, an incident such as Sandy Hook or the Uvalde School Shooting resulted in funding opportunities for organizations or even mandates to establish threat assessment in schools. While it is helpful to have these systems in place, multiple participants lamented about this reactive stance, wishing that the need for investment in smaller organizations or smaller communities could be realized before lives were lost.

**Finding 4: Funding discrepancies**

Funding mechanisms can vary widely from one legislation to the next, which is more dramatic at the local level. Some locations may mandate threat assessment programs, whereas others may have statutory training that is required regardless of budget shortcomings, meaning that threat assessment can become a last priority. Further discrepancies exist in funding availability; some may have funding available at the state level, whereas other communities must rely on federal funding structures. In addition, as one participant noted, even with federal and/or state funding, there is still likely to be some cost passed on to the local community, tying into the need for buy-in from smaller communities that may feel immune to dramatic threat events such as mass shootings. Existing funding concerns are further complicated by the demands of the given community. For example, one participant discussed the lack of mental health resources in their community and suggested this further compound challenges to threat assessment efforts.

The topic of funding among our local-level focus groups was often oriented around training; that is, training is expensive, must be provided consistently, and can be one of the first cuts to be made when budgets are tightened. This was different from our threat assessment practitioner interviews, where we found that training was a barrier but more so due to issues with buy-in and consistency over cost. This divergent finding is likely the result of the differences between the federal, state, and local funding infrastructure.

**Finding 5: Barriers are diverse**

Similar to findings from our practitioner interviews, the reported barriers to developing and maintaining a threat assessment team are diverse. Additionally, financial concerns are not the primary barrier
impacting threat assessment efforts. Every team included in our focus groups mentioned some level of barrier in their threat assessment process.

Figure 1. Word Frequency Cloud under the Barriers theme.

Listed barriers include community support and buy-in, finding the right people to do the work, training as a time commitment, inconsistencies in standards at the state and federal level, and the availability of resources, including financial resources but also access to training, access to employees, buy-in at multiple levels, and a lack of external resources such as mental health facilities that impact community threat assessment efforts. However, as illustrated in the word cloud above (Figure 1), these barriers ultimately come down to one thing: people. Whether it be buy-in by people or finding people to employ, the reported barriers are people problems. That is, tools and training are important but are not solutions without the buy-in and commitment of those around them.

While many of these findings again map to our findings from our practitioner interviews, a few are more specific to the focus group cohort. That is, not only is leadership and employee buy-in an important barrier to overcome, but our focus groups also raised the issue of community buy-in. This suggests that, at the local level, the surrounding community plays a more significant role in threat assessment overall than those existing at the federal level. In addition, community buy-in stands out as a different issue than that of employee or leadership buy-in—community members are not contained within a specific, related organization, for example, and the “stakes” are likely to be perceived as external and potentially even unrealistic, especially for smaller communities without a history of targeted violence or mass casualties.

Finding 6: Structured Professional Judgment Tools (SPJs)
Similar to our interview findings, WAVR-21 was the most frequently cited SPJ tool utilized by the teams included in our focus groups. However, only 3 of our focus groups mentioned the use of SPJs by their team. In addition, similarly to our primary interview finding, teams discussed individualized paths to finding best practices and available tools. One team, for instance, explained that they simply started Googling, and discovered the practice of threat assessment this way. They then adopted the FBI’s “11 Questions” for assessing school shooter threats and began using that as a tool. Another team was in the process of doing research on which tool to purchase and explained they were looking at three or four different companies at the time of documentation.

These findings suggest that tool usage among local teams is not widespread and that the existing knowledge base available to teams, especially those who are first establishing the practice, may be insufficient. Considering the consistency between our focus groups and practitioner interviews, these problems may pervade at both the local, state, and federal levels.
Finding 7: Insider threats are on the radar at the local level—at least for some
We were surprised to find that some of our teams were not only prepared internally for insider threats but brought the issue up without our prompting. While insider threat mitigation exists at the federal level, throughout the US Governmental structure, we did not expect the topic to arise during our focus groups. One team brought up the importance of considering insider threats while recalling an incident with a fired teacher who had committed arson. Another mentioned their insider threat program, while a third brought up the importance of insider threat mitigation across various levels of an organization. This finding suggests there is a demand for insider threat mitigation in smaller organizations and communities as well, and also suggests that some at the local level are aware of the importance of mitigating insiders in addition to external threats.

Supplemental Findings: Autocoded Themes
The autocoded themes provide some helpful additional insight. Most notable is the saliency of the “Community” theme. This aligns with our manual coding as well, which serves as a check on that coding. However, more importantly, it reflects the significance of the role that the surrounding community plays in supporting threat assessment at the local level. This is particularly noteworthy because, unlike several of our findings, this contrasts with our practitioner interviews. While buy-in among leadership was a frequent barrier reported in our interviews, the role of the surrounding community was rarely, if ever, brought up.

This contrast is most likely due to the nature of the different populations, and of relevance to this report; at the federal level, community buy-in is off the radar, because many of the federal institutions utilizing threat assessment do not engage with the community (for example, Department of Defense components are highly unlikely to engage with American citizens outside of the military population, as this is simply not their directive). However, at the local level, buy-in, while important at the leadership level, is framed as similarly important as community buy-in. In addition, local-level threat assessment teams rely on both reporting and information gathering from the community in which they are situated, demanding not only buy-in but engagement.

Another interesting contrast from our practitioner interview findings is the role of public health officials and the healthcare system in supporting threat assessment practices at the local level. Some lamented a lack of available health (notably, mental health) resources in their communities, while others discussed the importance of integrating mental health professionals into their threat assessment practices. This not only speaks to the importance of collaboration, as noted above, but also, what is seen as an important component of a multidisciplinary team. The emphasis on the importance of an interdisciplinary team for effective threat assessment and management is a theme that runs across our analyses and is often cited in the literature as well (e.g., Ellis et al., 2022).

Limitations Around Generalization
While our findings in this report are generally consistent with the findings across other components of our greater threat assessment work, we must note that our sample is limited and not representative. Therefore, our findings cannot be generalized to the greater population directly. Rather, these results should be seen as highlighting potential themes, issues, and real-world applications that are overlooked in the literature and in more systematic reviews. That is, this analysis provides a snapshot into the real-world threat assessment practices of teams at a range of state and local levels. This analysis further complements our Interview Report, which summarizes the findings across 13 interviews with threat assessment practitioners, mostly at the federal level.
Law Enforcement Interviews and Survey Instrument

In addition to the focus group analysis, we conducted a survey of law enforcement regarding their application of threat assessment in their job functions, which are discussed in more detail in this section.

Survey Sample

Data for this survey came from Prolific, an online platform that contains a database of potential research participants who have answered a host of demographic questions that allow researchers to narrow down their sampling. For this study, we were interested in the views of law enforcement officers. Our analytic sample contains 45 individuals of the 60 law enforcement officers in Prolific’s sampling database. While this sample is not representative of local law enforcement across the country (nor would it be feasible to conduct such a survey), we do see trends that align with prior findings, as well as saturation across many of our results, suggesting these responses provide an accurate snapshot of practices and pain points.

Survey Instrument

In the survey, we focused on triaging, reporting, SPJ/tool usage, and the pain points experienced. The survey measure questions are outlined below in Table 3.

Table 3. Survey Measures

<table>
<thead>
<tr>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a - What system do you currently use to take the public’s reports on threats</td>
</tr>
<tr>
<td>1b - What do you think works well with this system</td>
</tr>
<tr>
<td>1c - What do you think is the most efficient part of your current system</td>
</tr>
<tr>
<td>1d - What was most helpful in training on your current system</td>
</tr>
<tr>
<td>2a - What information is usually missing in reports you receive from the public</td>
</tr>
<tr>
<td>2b - Where do breakdowns tend to occur in the system you use</td>
</tr>
<tr>
<td>3a - How could a system to manage threats be improved</td>
</tr>
<tr>
<td>3b - What changes do you perceive to be most important</td>
</tr>
<tr>
<td>3c - What would you like to see in your ideal threat assessment software system</td>
</tr>
</tbody>
</table>

Findings

Threat Reporting Systems

When looking at reporting and triaging, we see a range of practices and programs utilized across LEOs in the survey sample. While the system Mark43 was the most frequently used, we also saw other programs utilized for reporting. These included: Watson, CLEMIS, JMS, SSPAN, and even Slack, a system designed for cloud-based team communication. Multiple agencies rely on local reporting, generally via 911 calls, school reports, and for one, Crimestoppers. Additionally, several rely on anonymous reporting lines, while others take a more hands-on approach by interacting with the community and scanning for potential threats by utilizing their existing data sources.

Moving on to what works well, LEOs in the survey sample largely agree that anonymous reporting, accessibility, and information sharing are critical to reporting systems. That is, the best reporting systems allow for anonymous reporting from the public, and are easily accessible, both by a range of
relevant parties, as well as by practitioners while in the field. Further, the automation of reporting services, such as auto-filling certain information and identifying trends and patterns. These responses are spread across participants. Most respondents further identified the streamlined nature of an electronic reporting system as a major factor in improving efficiency. These systems can collect information over time as well, allowing anyone who accesses them an in-depth view of a particular case, threat type, and so on, without needing to do targeted research to fill in those gaps. In short, automated reporting systems are widely regarded as improving efficiency and streamlining threat assessment processes.

Training has been a consistent theme across our threat assessment research. This includes the cost of training, the buy-in involved in supporting training, and personnel barriers. In our interviews with BTAM practitioners, many stated that working with law enforcement can be a challenge, as BTAM practices typically prioritize prevention through management efforts, whereas police training is often reactive and involves protecting public safety in real-time, with efforts typically ending with an arrest. As a result, these practitioners sometimes found themselves at odds with law enforcement in both collecting data and managing threats, due to the difference in approaches. Training was further identified as problematic if it was only offered once, rather than continuing education, and if it didn’t involve any tabletops of application. While not everyone in our sample had received specific training, those who did most frequently cited that regular practice and on-the-job training were the most helpful for them in their job duties.

What is Missing from Reports?
What is more noteworthy is what is identified as missing from these reporting schemas. One respondent summed up the issues noted across participants quite succinctly: “Who, What, When, Where, Why.” Most respondents identify missing crucial details. Timing and the location of potential events were also frequently cited. While some were attributed directly to anonymous reporting from the public, others explained that reporting agencies don’t always provide useful information, such as screenshots of threats, in addition to other identifying information. Respondents went on to identify where breakdowns primarily occurred, finding that getting information to the correct people in a timely fashion often poses a challenge across systems. Another breakdown can occur when different organizations are utilizing different reporting software or programs, resulting in a fracture in the flow of information. Across responses, cross-reporting, communications, and reporting delays were the most frequently cited breakdowns in the process, indicating specific areas for improvement in future reporting systems.

Recommendations for System Improvement
Most of the suggestions we received focused on increasing communication between agencies/departments and expanding reporting features from the public to capture more data, with particular emphasis on the first suggestion. That is, an ability to coordinate with fellow law enforcement agencies and other related organizations appears to be a challenge for many. Given the range of systems and programs in place, this is not in itself surprising. However, given the nature of threat events, timely data sharing and communication with other law enforcement is often a crucial component in staying left of boom.
Figure 3. Word cloud of question 3a – ‘How could a system to manage threats be improved?’

A word frequency cloud, depicted above in Figure 3, provides an overview of the range of responses we received. While there were consistent themes across multiple response groups, opinions on improvement covered a range of topics. One respondent simply stated, “I have no idea, it’s above my pay grade.” Another, however, suggested that they would “love to see an auto dispatch feature with GPS functionality,” which is a specific set of technological advances. This stands in contrast with another who stated, “Experienced leadership training, running system.” This addresses an entirely different pain point, and while it may speak to a specific dispute or lack of leadership in that respondent’s department, it raises an important point about the role of leadership in effective threat assessment. However, there are three loose themes across the responses: community engagement, access and sharing information across departments/agencies, and improving communication at all levels.

These themes pop up repeatedly across the analysis. It seems clear that, at the local level, one of the greatest challenges or pain points is coordination across or between agencies. While departments such as Joint Terrorism Task Forces (JTTFs), are designed to help improve information sharing between agencies, it may be that lower-level threats or threats unrelated to terrorism do not make it to that level of scrutiny. It may also be that at the beginning of the process, such as when a potential threat is first reported to an agency, it must first move up through the assessment and management process to be on the JTTFs radar. Whatever the case, there is widespread agreement that challenges in communication and data sharing at the local level continue to be a barrier for local law enforcement. Multiple respondents suggested the ability to access other agencies’ threat assessments and reports. With the range of reporting systems in place, however, this would be a challenge.

Another important theme is the ability to both obtain information from and share information with the general public. This points to our earlier finding about the role of the community in effective threat assessment. Without members of a community reporting potential threats, there are limited means for law enforcement to become aware of a potential threat before a threat event comes to the attention of the police. Some feel the community should be made aware of potential threats, while others simply want more engagement with reporting and providing data. This involves both education regarding what information is most pertinent and how to properly convey concerns. However, multiple respondents also suggested potential victims or the local community should be more informed about potential threats.
These themes were largely repeated when we asked what changes were perceived as most important. In addition, however, we received quite a few suggestions about technical aspects of the reporting process. One suggested more advanced visualization tools while another suggested a larger, more spread-out format, to make the process of reporting simpler.

Finally, we asked about the respondents’ ideal system. At this point, some of the answers had become redundant. However, a handful of respondents stood out with extensive suggestions. A few choice selections will be provided below:

- **A system should be able to easily verify if a threat is credible.** The system should allow for all the threats to be saved. I want other agencies to view/share the threat and be able to update that threat. It would be great if a picture of the suspect could be added to the system.
- **A large interconnected information hub that would distribute important detailed information to all relevant agencies, teams, and individuals in real time.**
- **Any software that can pick up on trends in location, suspect, or other repeated information would be helpful.** Elevated or time-sensitive threats should have a way to get to supervisors immediately.
- **Ease of use and intuitive feel.** A layman who needs to use it should be able to manage it when necessary, even if they have no specific training on the system.

Again, the ability to communicate and share potential threats across agencies is highlighted. Accessibility is also raised here in terms of ease of use and timeliness. In addition, multiple respondents suggested that some form of trend analysis or chronology of threats would be beneficial, both here and across other responses.

**Conclusions**

**Communications and Collaboration**

Our primary takeaway from this report is that effective communication and collaboration across agencies and entities, as well as within, is crucial to effective threat assessment and management. This is especially noteworthy regarding the collaboration between various governmental and related agencies and the local police, as well as student resources officers. Having and maintaining relationships with the police allows auxiliary threat assessment teams to act swiftly and in a coordinated fashion. However, there are challenges here as well—law enforcement carries its own culture, that at times clashes with those on more traditional threat assessment teams, such as those local school districts or university settings. As a result, it takes a willingness from both parties to meet in the middle, which at times, comes down to having the right person in the role.

However, for there to be effective collaboration on threat assessment efforts, there also needs to be effective communication structures, especially between various levels of law enforcement. This includes both regional law enforcement communicating with the state level, as well as coordinating across entities for both information sharing and gathering. Infrastructure that facilitates real-time information sharing between agencies is a first step. However, this is a challenge, given the range of reporting systems and threat assessment structures across agencies. The ability to cross-reference a potential threat with neighboring agencies, for example, may provide important context in both assessing and managing that threat. Therefore, effective communication—and an existing infrastructure to support it—remains a struggle for many local law enforcement that we sampled. This is particularly important at the reporting stage, as this is where the most pain points were identified.
The Community
Of particular note is the role that the community plays in shaping local threat assessment practices. This was a prominent theme across both our manual and auto coding – and stands in contrast with the findings from our practitioner interviews. At the local level, the community functions in three important ways: first, they are often the entry point for cases through reporting functions. Second, threat assessment teams rely on the community to gather information during the assessment process. Finally, buy-in from the community is oftentimes essential for both securing funding as well as mitigating the other two aforementioned community factors. In short, the more informed the community surrounding a threat assessment team is, the more beneficial that community can be to the process, and, in turn, that team is better able to manage and mitigate threats.

The theme of incorporating the community also arose during our survey. Many agencies report that they would like to expand the community’s ability to report, either by making it more accessible or allowing for more data points. On that note, however, there is a to educate the community on what is worthy of reporting and what details are needed to effectively manage a threat. Many suggested the ability to report images, as well as potentially automatically check the validity of phone numbers and other identifying information included in reports. Taken collectively, this suggests that law enforcement relies on the community for reporting, but that barriers to effective reporting at the local level exist, even when anonymous reporting lines or apps are available. In part, educational efforts to inform the public about what constitutes a potential threat and what information should be included in a report are an important first step.

Although the federal level also relies on tips from the public, there is simply less variation in the method of reporting and the reporting agency. That is, it is not difficult for a citizen to search online to make a report to the FBI, but within a local community, figuring out the how and who is more of a struggle. One must determine, for instance, if they are to contact the county police versus state law enforcement.

It may be that smaller, more locally-oriented teams and organizations are better able to rely on informal relationships with police, within the community, and with related stakeholders. Regardless, it is likely that the size of the team helps determine reliance on community ties and existing relationships with police. While further research can attempt to tease out these differences, the lesson stands that general awareness about the purpose and benefits of threat assessment can help all levels of the process, from community to leader buy-in and engagement. In addition, a community-oriented approach is a logical one, regardless of the community in which it is situated. This is the same lesson that community-oriented policing teaches us—to serve a community, one must be integrated within that community.

Takeaways
Ultimately, we find similar themes to findings across federal threat assessment practices. Buy-in is crucial for effective threat assessment, from leadership and across teams, as is the need for collaboration between different agencies and organizations. However, there are a few departure points from our general findings.

First is the importance of both informing and including the community in the process. Some departments suggested they would like to inform local communities about potential threats. Those who had locally oriented anonymous reporting systems generally found them to be effective, though they also often suggest a need for more robust data when reporting. Law enforcement and the community in which they are situated is our first defense against any major threat event. An informed community with a straightforward reporting system that is well-advertised locally will be better positioned to prevent and manage those threats.
Additionally, there continue to be pain points at the local level that may prove a barrier to effective prevention and management. That is, the variation and at times, lack of collaboration across agencies in each locale is still a frequently cited barrier to information sharing and gathering. One large population center may contain multiple law enforcement departments, tasked with protecting spaces nearby. In short, communities aren’t always drawn around a jurisdiction, such as a county line or a suburb of a city, and law enforcement needs to be able to coordinate and communicate with other regional departments to provide both history and appropriate context for a potential threat actor. For example, someone may cause concern both at work and at home, yet those locations may be in separate geographic jurisdictions. In cases of a population center with multiple jurisdictions, especially, an infrastructure for information sharing, communication, and collaboration across those agencies will help provide a more robust threat prevention and mitigation framework in a given community.
Blind Spot C: Reducing External Threat Fixation – A Necessary Refocusing on Insider Threat

The third blind spot involves removing a fixation with external threats that individuals conducting threat assessment tend to have. To do this, a multi-disciplinary approach to threat assessment from an insider threat perspective was explored.
Examining Best Practices in Threat Assessment from an Insider Threat Perspective:
A Review and Integration

NCITE Center Research Team
Matt Allen – University of Nebraska at Omaha
Kat Parsons – University of Nebraska at Omaha
Tin Nguyen – University of Nebraska at Omaha
Lauren Zimmerman – University of Nebraska at Omaha
Introduction
The purpose of this report is to examine behavioral threat assessment from an insider threat perspective through an extant literature review. Broadly defined, insider threats generally refer to individuals, such as employees, contractors, or former employees, with privileged access to organizational information, locations, or systems who have the potential to cause harm. These threats can be intentional (malicious) or unintentional (non-malicious), with intentional threats being of most interest to the current purpose. These intentional threats can be further categorized into specific threat incidents or outcomes, such as sabotage, theft of intellectual property, fraud, espionage, and targeted violence. This contrasts with behavioral threat assessment (often referred to simply as “threat assessment,” used for the remainder of the report), which is typically concerned with understanding potential threats of violence in different settings (Meloy et al., 2021).

Both definitions consider the threat that an individual actor (rather than a group) poses, but the definition of “insider threat” is broader in the sense of the outcomes and targets considered. Specifically, definitions of insider threat consider threats to individuals, systems, and the larger organization. “Threat assessment,” while largely concerned with physical harm to individuals, is broader in the sense of context, which includes additional locations such as public places and schools in addition to the workplace. Threat assessment also includes special consideration of targets, such as intimate partners and public figures. These similarities and differences are illustrated in Figure 1.

![Venn Diagram of Threat Assessment and Insider Threat Practice Areas](image)

**Figure 1. Venn Diagram of Threat Assessment and Insider Threat Practice Areas**

There are several reasons to examine threat assessment from an insider threat perspective:

- **The extant insider threat literature draws on different disciplines than what is typically found in the threat assessment literature.** As illustrated in Figure 2, insider threat has emerged as an area of concern more recently compared to threat assessment, driven by (a) high-profile espionage insider threat cases in the U.S. federal government (e.g., Robert Hanssen⁴), (b) the emergence of computer technology as an opportunity for malicious insiders to cause significant harm with relative ease (Pfleeger & Caputo, 2012), and (c) the increasing costs of insider threat incidents to organizations (e.g., IBM Security, 2020; Ponemon Institute, 2022).

---

³ See, for example, the National Insider Threat Task Force [NITTF] mission fact sheet, insider threat training provided by the Center for Development of Security Excellence [CDSE], and the Cybersecurity & Infrastructure Security Agency’s [CISA] insider threats page.

⁴ [https://www.fbi.gov/history/famouscases/robert-hanssen](https://www.fbi.gov/history/famouscases/robert-hanssen)
Specifically, there is a substantial information security/cybersecurity literature examining types, antecedents, and interventions of insider threat incidents (see Homoliak et al., 2019 for a review), and using these examinations to develop testable models for predicting and preventing such incidents (see Bedford & van der Laan, 2021; Greitzer et al., 2019; Lenzenweger & Shaw, 2022; and Witty, 2021, for examples). Thus, there are models and empirical data available in the insider threat literature that may inform the practice of threat assessment.

- **Insider threats are studied in an organizational context.** The organizational context has several benefits. First, as alluded to in the previous point, there are data available in organizational contexts that are not readily available in other settings, such as schools and public places. For example, organizations routinely collect data on individual differences (e.g., through pre-employment assessments, and training), behavior on the job (e.g., through performance reviews, citations for rule violations, absences), and behavior on organizational networks (e.g., attempts to gain unauthorized access, activity logs). Consequently, models of insider threat and associated interventions tend to be more specified and have more empirical support than their threat assessment counterparts. While there is no oneto-one correspondence between insider threat and physical violence in other settings, a deeper understanding of the insider threat perspective allows us to examine promising avenues for understanding threat assessment more generally.

A second benefit of the organizational context is the ability to leverage organizational sciences, such as economics, industrial/organizational psychology, and management, to further inform counter-insider threat theory and practice (Dalal et al., 2022). Insider threat researchers and practitioners have begun to recognize the limitations of an exclusively command and control approach (i.e., focused on compliance and external controls) in countering insider threats, and the potential impact of positive incentives in reducing the probability of threat incidents (Baweja et al., 2022; Moore et al., 2016; 2022). Organizational scientists have studied these positive deterrence (i.e., those that increase employee job satisfaction, wellbeing, and performance) factors for decades and are thus well-suited to inform current practice.

---

5 "The Google Ngram Viewer displays user-selected words or phrases (ngrams) in a graph that shows how those phrases have occurred in a corpus. Google Ngram Viewer’s corpus is made up of the scanned books available in Google Books." Source: https://infoguides.gmu.edu/textanalysistools/ngram#:~:text=About%20Google%20Ngram%20Viewer,books%20available%20in%20Google%20Books.
• Threat assessment practitioners recognize the role of insider threats. According to recent interviews with 13 threat assessment professionals (NCITE, 2022a), insider threats are relevant to the work done by threat assessment teams in at least three ways. First, insider threat teams tracking network behavior can refer employees exhibiting virtual behaviors of concern to threat assessment teams for follow-up. Second, threat assessment teams can refer employees exhibiting behaviors of concern for additional monitoring, particularly in cases where the individual of concern has the opportunity and capability to retaliate to a perceived grievance via cyberattack. Third, threat assessment teams are frequently working with insiders and thus should be aware of any special considerations or data sources that can be leveraged in their assessment.

In summary, much can be gained by examining threat assessment from an insider threat perspective and by incorporating related literature areas. To realize these gains, the report contains the following sections:

Part 1: Insider Threat Literature Review.
In this section, we begin with a brief overview of the counter-insider threat research and models of insider threat. This helps to situate the remainder of the report in the larger context of this literature. In particular, it contextualizes our emphasis in the remainder of the report on three types of malicious insider threats of particular interest to public sector entities – espionage, sabotage, and workplace violence – as they are most relevant to the threat assessment context. We conclude this section with a discussion of the limitations of the insider threat literature when applied to threat assessment practice.

Part 2: Literature Related to Insider Threat.
We build off Part 1 by supplementing the counter-insider threat research with relevant (a) security and (b) social and behavioral science literature. The social and behavioral sciences section applies lessons learned from a range of disciplines, including criminology, psychology, and management, to the question of how malicious insiders can be better detected and deterred.

Conclusion and Next Steps.
The current report summarizes the literature that we are drawing upon to develop new insights related to insider threat. In this section, we will summarize key conclusions at a high level and describe the next steps underway in this effort.

Part 1: Insider Threat Literature Review
Our first step in this research was to obtain a broad-based understanding of extant insider threat literature. Specifically, our goal was to obtain peer-reviewed research articles to answer the following two questions:

• How is insider threat understood and operationalized?
• What predictive models exist for insider threat, and how are those structured?

To accomplish this, we searched several research databases\(^5\) using the following Boolean phrase as a search starting point: (“insider threat” OR “insider risk”) AND (“model” OR “framework” OR “typology” OR “paradigm” OR “category” OR “taxonomy” OR “ontology” OR “predict” OR “mediation” OR “moderation” OR “critical pathway”). After the initial search, restrictions were excluded from the

\(^5\) IEEE Xplore, ACM Digital Library, PsychInfo, ABI/INFORM Global, Criminal Justice Abstracts, ProQuest Academic Complete; others searched yielded no results
search of social and behavioral science databases (e.g., PsycINFO) as the initial search yielded very few or no articles.

We supplemented this search with known research-backed industry resources for answering these questions, such as the technical reports found on the websites for the Defense Personnel and Security Research Center (PERSEREC)⁷ and Carnegie Mellon University’s Software Engineering Institute (SEI, specifically the CERT Division)⁸. As expected, the vast majority of articles came from information security/cybersecurity or similarly situated resources. Given this finding, the remainder of this section summarizing definitions and models of insider threat heavily emphasizes that literature.

Defining Insider Threats
Due to shifts in the workplace, such as from physical to digital storage and from manual to knowledge work, the study of insider threat is prevalent in the information systems and technologies (IS&T) field, including IT and cybersecurity. Indeed, the term “insider threat” gained prominence in the industry due to data breaches from malicious insiders (Capelli et al., 2012). There are several definitions of insider threat in the IS&T literature, which vary on (a) definitions of an “insider”, (b) consideration of maliciousness, and (c) treatment of access. See Appendix A for some example definitions and Homoliak and colleagues (2019) for a review.

Defining an “Insider”
Definitions of insider threat vary regarding who qualifies as an insider (see Appendix A for example definitions). Because information technology is digital (and therefore easily sharable), it is possible when collaborating to easily share documents or provide access to those outside the company. Some definitions are concerned only with those who are employees, while others see anyone who was given access to a system (e.g., a contractor) as an insider. For example, Butts and colleagues (2005) define an insider as “... any individual who has been granted any level of trust in an information system” (p. 413). Others provide more specificity, ranging from, “a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization’s structure” (Bishop et al., 2008; p. 5) to more technical definitions, such as, “an individual who has the knowledge of the organization’s information system structure to which he/she has authorized access and who knows the underlying network topologies of the organization’s information systems” (p. 240; Althebyan & Panda, 2007).

Maliciousness
One way to categorize insiders is by intent—malicious vs. negligent (Bailey et al., 2018; Carlson, 2020). Malicious insiders are those who, “intentionally used ... access... that negatively affected ... the organization’s information or information systems” (Costa et al., 2016; p. 1). While negligent insiders are typically considered unintentional (i.e., non-malicious), some insiders, such as those accessing unauthorized information to satisfy a curiosity, can be both negligent and malicious if the accessed information is then part of a threat event. Bailey et al. (2018) illustrate this situation in their analysis of the Vocabulary for Event Recording and Incident Sharing (VERIS) database, where 44 percent of the insider-related breaches were rooted in negligence or co-opting of organizational resources. They demonstrate how a negligent insider may not intend to cause harm to the company but may instead use their access for their own self-interests, such as accessing client records to get contact information to ask an individual out on a date. Another way to understand intent is through the end goal of the action. Band et al. (2006) see actions against the IT systems as either insider sabotage or espionage—is the

⁷ https://www.dhramil/PERSEREC/SelectedReports/
⁸ https://www.sei.cmu.edu/publications/technicalpapers/index.cfm
insider hoping to harm the organization for their own interests (sabotage) or are they working on behalf of another party (espionage)? Some scholars further distinguish these incidents more by separating IT sabotage, theft of intellectual property, and fraud (Capelli et al., 2012). Others disagree with using insider threat as an umbrella under which sabotage and espionage fall under, instead separate espionage, sabotage, and insider threat into their own categories while acknowledging that there may be overlap (Bulling et al., 2008).

Access
A second way to categorize insiders is the route taken to access a system. Alawneh and Abbadi (2011) understand this as whether the access credentials were obtained through authorized or unauthorized means, and whether the access to a system was legitimate. The authorization of credentials is whether the organization gave the insider the credentials or not, whereas the legitimate access is whether the insider was supposed to use their credentials to access that system or not. Another way of thinking about this is that some researchers focus on whether the insider stole the key to access a room or if it was given to them by the organization (Alawneh & Abbadi, 2011), while others are interested in if the insider was supposed to use their key to open that door or not, or even be in the room at all (Bishop and Gates, 2008; Elmraït et al., 2015). An extension of this category is the type of insider and their authorization level.

Summary
As described above, definitions of insider threat tend to vary in terms of (a) “insider” definition, (b) maliciousness, and (c) access. In general, older definitions of insider threat contain more specificity while more recent definitions tend to be more inclusive. For example, SEI CERT’s definition of an insider shifted from, “A current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data,” to “an individual who has or had authorized access to an organization’s assets” in recent years (Zimmer et al., 2022; p. 2:3). Similarly, older definitions of insider threat focus more on violations of IT security policies (e.g., Bishop, 2005; Bishop & Gates, 2008; Theoharidou et al., 2005). However, a consistent element across definitions is the insider misusing their privileges, to potentially include unintentional acts (Elmraït et al., 2020; Greitzer et al., 2016).

Based on the above, we can conclude the following:

- **Defining “insider threat” is complex.** Several elements impact how insider threat is defined. Recent definitions have generally become more inclusive to incorporate the full range of potential individuals and expressions of insider threat.

- **There are several ways to define insiders and insider threats.** That said, we agree with the more general definitions, such as those provided by the National Insider Threat Task Force (NITTF) (see Appendix A). However, while this general definition covers the full threat landscape, our analysis for the remainder of the paper will focus on malicious (as opposed to negligent/non-malicious) insiders with privileged access to government (as opposed to private sector) resources.

With a working definition of insider threat in hand, we turn our attention to IS&T-oriented models to predict insider threats and threat events.

**Models of Insider Threat**
A foundational model for determining insider threat risk is referred to as the “critical pathway” model. Shaw and Sellers (2015), in their description of the model, posited, based on empirical insider threat research, “that there exists a common set of factors and a similar pattern of individual and
organizational behavior across the many occurrences during recent years” (p. 1). This model suggests that factors, including personal predispositions, personal and professional stressors, concerning behaviors, and problematic organizational responses increase the probability of a hostile act. The last factor (problematic organizational responses) is particularly critical in this model, as adaptive or maladaptive responses by the organization can increase or reduce the probability of a threat event. Another notable feature of the model is that it considers the complexity of human behavior in making judgments, making it a good foundation for Structure Professional Judgment (SPJ) tools (Lenzenweger & Shaw, 2022). This model has proved foundational in the scholarship and practice around insider threat and is illustrated in Figure 3.

![Figure 3. Graphical Representation of the Critical Pathway Model](image)

However, the critical path model is not without criticisms or limitations, as discussed recently by Lenzenweger and Shaw (2022). For example, empirical validation of the model remains limited (though efforts to collect data to bolster the evidence are underway), and questions remain regarding, among others, (a) methods empirically combining risk factors to develop risk profiles, (b) methods of “offboarding” individuals currently on the critical path, and (c) potential interactions among variables in the model. Despite these limitations, the critical pathway model remains foundational for those looking to understand the human element of insider threat risk.

Bedford and van der Laan (2020) describe several models of varying degrees of specificity, including the critical path model. They note that while earlier models focused on individual risk factors and technically-oriented solutions (e.g., access controls), recent models have sought to better capture the interplay between employees and their environment. Recognizing this, Predd and colleagues (2008) considered the role of the individual in the context of the organization (i.e., expressed policies), the system (i.e., implied policy), and the environment (e.g., economic). This attempts to situate threat events in a more contextual light, including whether an insider’s actions were legal, the type of organizational

---

9 Version of the model derived primarily from Noonan (2018).
policies in place, and the motives of the insider. While these authors considered this issue from a high-level, others have examined the unique interactions of some of the elements of this model more deeply.

For example, Greitzer and colleagues (2016; 2019; 2021) developed and validated (using expert judgment to inform Bayesian estimates) a comprehensive ontology for predicting insider threat risk. The hierarchical Sociotechnical and Organizational Factors for Insider Threat (SOFIT) ontology includes factors (individual, organizational), classes, subclasses, and observable indicators. For example, one of the classes within the individual factor is *job performance*, which can be further broken down into subclasses such as *cyberloafing* and *negative evaluation*. Within the negative evaluation, for example, indicators might be *performance below expectation, complaints, or missed deadlines* (Greitzer et al., 2019). Similarly, Legg et al. (2013) proposed a conceptual model for insider threat detection with four categories of elements, including enterprise (e.g., organizational policies, business processes), people, technology, and information, and physical (e.g., access controls, and security surveillance). These models are notable for several reasons but are highlighted for our purposes because they (a) explicitly include organizational contextual factors, such as poor supervisor-employee relations or work conditions, in addition to individual and technical factors, and (b) are designed to help make predictions about the risk of a threat event.

Despite their strengths, the lack of external validation of these models is a key criticism from some authors, as is the observation that they can be difficult for practitioners to apply due to their complexity (Bedford & van der Laan, 2021; Schoenherr & Thompson, 2020). To address concerns about these and other models of insider threat, Schoenherr and Thomson (2020) proposed a model to differentiate employee actions and identify specific forms of insider threat. The model, SIEVE (severity, form of employee norm violation, intentionality, and ethicality), seeks to classify individual behaviors based on motivations to develop better monitoring and intervention frameworks. Nostro and colleagues (2014) also focus on the motivations and opportunities of potential insiders by exploring the unique access that a given role may have and the attack pathways they may take. Sokolowski, Banks, Dover (2016) explore an agent-based model (i.e., how individuals interact with larger systems), but focus on the complex adaptive behavior of an individual, incorporating different motivations and organizational factors.

This set of complex intersecting factors has led to the development of integrated insider threat frameworks that go beyond traditional network monitoring and security procedures. For example, Bedford and van der Laan (2021) developed the Organizational Vulnerability to Intentional Insider Threat (OVIT) survey to describe factors that increase insider threat risk, with individual, organizational, and technical dimensions included. This model is notable because the derived measure can be used as a validation tool for evaluating new interventions. Whitty (2021), based on the coding of case studies derived from interviews with industry professionals, developed a model that incorporates practices such as hiring/pre-screening, improving the workplace culture, and so forth. This model is notable for its explicit inclusion of potential prevention factors. Finally, Elmrabit and colleagues (2020), building off Greitzer’s work cited above, incorporate preventative factors into a detailed model of insider threat risk predictions. Graphical representations of all three models can be found in Appendix B.

**Methods for Detecting Insider Threats**

Techniques for detecting insiders are frequently classified into one of three categories—technical, non-technical, or a blend of the two (see Homoliak et al., 2019 for a more complete review). Early information security research recognized that technical solutions alone were insufficient for detecting and mitigating insider threat risk (e.g., Pfeeger & Caputo, 2011; Steele & Wargo, 2007). The methods of detection offered in the technical fields differ in their plans, implementation, and what they are hoping
to capture. Most solutions end up being reactive, but some try to be predictive. Some act as decision support systems to aid human judgment, while others are meant to operate largely autonomously.

A basic example of a technical solution is the proposition for a predictive system that flags those who are in the initial pathways of the insider threat cycle, specifically those who are accessing parts of the organization’s computer system that they are not supposed to. These systems are based on permissions (are they supposed to be accessing this content) or expected job requirements (is accessing this content a normal part of their job). However, technical solutions can get more complex. For example, intrusion detection systems are deployed within a system to determine if there has been any intrusion from outside (Elmrabit et al., 2020). Intrusion detection can be executed in several ways. Artificial Neural Networks (ANNs) have been suggested as one solution, where a system will be trained to become familiar with normal work patterns and then be able to recognize and flag anything out of the norm (Williams et al., 2021).

In terms of non-technical solutions, common techniques include (a) policies (e.g., IT and HR policies), (b) personnel training (e.g., security awareness), and (c) psychological prediction (Elmrabit et al., 2020). “Psychological prediction” refers to characteristics that personnel around an insider will recognize and report. Maasberg et al. (2020), for example, have identified and empirically validated a set of observable behaviors associated with malicious insider threats. Bailey et al. (2018) discuss how HR and management could flag behavior from those they oversee and investigate as needed. Managers in this case need to be properly trained and have the time, resources, and familiarity with those they manage to be able to notice and flag concerning behavior.

Blended solutions combine policy and technical solutions, such as digital rights management, which can be seen in practices like deactivating work accounts and withdrawing credentials as soon as someone quits or is fired (Alawnhe & Abbadi, 2011; Elmrabit et al., 2020; Silowash, 2013). Withdrawing credentials is just as important, if not more, for those who are working outside the organization (e.g., contractors) and have been given access to support the organization as they are an easy element to overlook. These contractors may not have a distinct termination moment, making it easy to forget to pull credentials. Another form of digital rights management is group-based or role-based access control. These are systems that allow certain individuals or job roles (such as a systems’ administrator) to access specific files. This allows the narrowing of the scope of those who have access to the files, particularly if they are sensitive ones. This system helps protect critical files from modification, deletion, or unauthorized disclosure (Silowash, 2013).

We turn next to the implications of this literature for a better understanding of espionage, sabotage, and workplace violence from a threat assessment perspective.

**Key Takeaways from Part 1**

From the above literature review, we can conclude the following regarding the insider threat literature as it relates to threat assessment.

**Takeaway 1: The insider threat literature includes detailed ontologies and testable, data-backed predictive models.**

Thus, these models can be very helpful in gaining a better understanding of the complex interplay of factors (e.g., personal predispositions, organizational, management actions, stressors) in support of threat assessment practice. For example, these models could help to enrich existing Structured Professional Judgment (SPJ) tools with (a) the identification of new indicators, (b) enhanced descriptions
of existing indicators, or (c) data to inform the potential weighting of indicators to support professional judgments.

However, as it relates to their application to threat assessment, these models are not without limitations. First, the level of specification of many of these models creates a challenge for non-technical professionals to use in a meaningful way to inform practice. This is not surprising given the field they came from—the complexity of these models is not a problem for machine-managed systems. However, translation will be required to help inform practice and policy. Second, most of the models of insider threat described above focus on “lone actors.” Multi-actor threats are not considered in most of these models even though Whitty (2021) found that 32% of insider threat cases in her study involved multiple actors. Most of the cases in this study were of fraud attacks, but the lack of consideration of multiple individuals working together is an oversight that should be built into any model. Finally, our literature review yielded very little information about the intersection between different types of security teams, such as cybersecurity, physical security, and other protective services. Better practices regarding the intersection of different security functions and related functions such as HR did emerge in our interviews with 13 threat assessment professionals (NCITE, 2022a), suggesting more work is needed.

**IMPLICATIONS OF TAKEAWAY 1:**

Insider threat models can be leveraged to inform threat assessment practice, but new literature must be added to enhance applicability (e.g., the role that groups might play in insider threat). We address this implication in Part 2 by identifying other literature that can build on current research related to insider threat.

**Takeaway 2: Definitions of insider threat, even when narrowed to malicious insiders, include a broad range of potential outcomes.**

As described above, early IS&T insider threat research focused narrowly on IT security violations. The expansion of the definition to capture other outcomes (e.g., fraud, workplace violence) requires corresponding enhancement of practice to consider off and on-network behaviors. Some indicators thought to be predictive of insider threat are, for several reasons, difficult to measure using network monitoring tools. For example, personal dispositions related to life events (e.g., marital problems) are not always easy to collect due to availability and/or ethical considerations. While HR and security technologies have increased employee monitoring capabilities, not all organizations will be comfortable with their use. Additionally, on-network indicators will be less relevant for certain types of organizations, such as mid-sized companies or companies where much of the work is done off-network.

The range of outcomes and complexity in potential sources of data suggests more nuance may be needed in the models. The models referenced previously are designed to predict all types of outcomes, even though certain indicators may be highly relevant for certain outcomes and much less so than others. In reality, there may be multiple “pathways” to a threat event rather than one “critical” pathway. The idea of defining multiple pathways is not a new one. Lenzenweger and Shaw (2022), in discussing future directions of the original critical pathway model, suggest that identifying additional pathways would be a good enhancement of the original model. Whitty (2021) proposed several pathways to becoming an insider threat, such as “the addict,” “pure greed,” and “disgruntled employee.” Finally, Shoennehr, Lilja-Lolax, and Gjoe (2022), propose a multiple-pathway approach to understanding social identities and motivations of threat actors that yields three general pathways: unintentional, ambivalent, and intentional.
**IMPLICATIONS OF TAKEAWAY 2:**
The foregoing suggests that, when considering models of espionage, sabotage, and workplace violence, it may be beneficial to start with a grounded theoretical approach that can be applied to a wide variety of contexts, with a particular emphasis on potential pathways.

**Takeaway 3: Most proposed methods for mitigating insider threat risk focus on technical solutions to predict or catch an individual in an act of wrongdoing.**
Given the IS&T focus on network security, it is not surprising that the literature would emphasize technological solutions. However, as pointed out by others (e.g., Lang, 2022; Lenzenweger & Shaw, 2022), ideally mechanisms would be in place to prevent individuals from seriously considering an insider threat event in the first place (i.e., providing an “off-ramp” to those on the critical path). This could come in the form of deterrence or employee support strategies that add resilience to the system. While human and organizational factors feature prominently in the above-referenced models, they are treated primarily as data points to be used to inform risk profiles. There are opportunities to better leverage our understanding of these features in support of other, more preventative, policy initiatives, such as effective organizational leadership, codes of conduct, and employee assistance programs (Baweja et al., 2022).

**IMPLICATION OF TAKEAWAY 3:**
When considering insider threat mitigation (or reduction of insider threat risk), strategies to “positively deter” (Moore et al., 2016; 2022) or “off-ramp” individuals from the critical path toward malicious activity should be explicitly incorporated into any recommendations. We discuss the theoretical underpinnings of potential positive deterrence in Part 2.

**Takeaway 4: The mechanism for applying general insider threat models to specific organizations is not always clear.**
Related to takeaway 2, it is not always readily apparent how the above-referenced insider threat models apply to specific organizational contexts. For example, the Greitzer et al. (2019; 2021) SOFIT model proposes specific indicators to be included in the model, but the specific metric/tool for populating that indicator is left to the organization. Implementation tools and guidelines are needed to bridge the gap between theory and practice. For example, the nature of the indicators, threat landscape, and types of people working in a specific job will depend on the job demand characteristics. Jobs can vary greatly on job context dimensions, such as degree of human interaction, physical work conditions, physical requirements, job hazards, degree of structure and responsibility, and so forth (Morgeson & Humphrey, 2006). All of these may significantly impact (a) the manifestations of specific indicators and (b) their efficacy in predicting a threat event. Furthermore, it also changes the nature of potential malicious insiders themselves. To take an obvious example, kinetic workplace violence is unlikely to be a concern in a virtual financial services company, but fraud may be a significant concern. Certain fields also have specific demand characteristics, suggesting we would also expect to see differences in types of insider threat by discipline. Thus, comprehensive models of insider threat must also include mechanisms for “personalization” to the organizational context.

A final point related to this takeaway—assuming organizations do take action to mitigate potential insider threats, how can an organization determine whether it yielded a positive outcome? Because insider threat is a low base rate event, “absence of an incident” is not likely to be a particularly useful metric. This suggests the need to develop criterion measures for validating insider threat risk based on indicators—the goal of insider threat mitigation policies then would be to have a positive effect on these
indicators. Bedford and van der Laan’s (2021) OVIT survey provides a useful starting point for addressing this gap.

**IMPLICATION OF TAKEAWAY 4:**  
When considering insider threat mitigation (or reduction of insider threat risk), strategies to contextualize general models to specific organizational contexts should be considered.

**Part 2: Literature Related to Insider Threat**

As described in Part 1, most research classified specifically as “insider threat” comes from the information systems and technologies (IS&T) domain. However, other resources may also be brought to bear on the topic of insider threat as it relates to threat assessment. Our objective in this section is to gain a more complete understanding of insider threat antecedents and contextual factors from multiple perspectives. Thus, we distinguish among two types of resources in this section: (a) practitioner-oriented and (b) social and behavioral science. “Practitioner-oriented resources” refer to non-information security publications to assist professionals in a variety of domains (e.g., security professionals, managers, HR practitioners) in mitigating insider threat risk. In our review, we identified practitioner-focused resources for mitigating espionage, sabotage, and workplace violence. Next, relying on the authors’ expertise, we identified several social and behavioral science domains adjacent or related to the topic of insider threat. This includes political violence, preventing terrorism and targeted violence, counterproductive work behaviors, and organizational adaptability. For these sections, we relied on canonical articles to survey the literature and how each might be brought to bear on the topic of insider threat.

**Practitioner-Oriented Resources**

In the next three subsections, we describe practitioner-oriented resources for the three types of insider threats identified to be of most interest to the current context—espionage, sabotage, and workplace violence. We focus on practitioner-oriented resources as the academic literature is touched on in other sections of the current report. This also helps to ground the remainder of the paper in the context of current best practice recommendations.

**Espionage**

Organizations now face challenges of an increasingly cyber-connected world, with technology often moving faster than policymakers can keep up. This is commonly referred to as the “pacing problem,” first outlined by Larry Downes in his 2009 book *The Laws of Disruption* and with the now-famous quote: “Technology changes exponentially, but social, economic, and legal systems change incrementally” (p. 2). One recent example of this problem emerging is in the use of facial recognition software. Despite widespread use by law enforcement and beyond, the entire state of California recently banned its use of police-worn body cameras (Merken, 2019). This demonstrates not only the inconsistent regulations of new technologies between states but also exposes the fact that new technologies (such as facial recognition software on body cameras) are both available and widespread without any consistent regulations. In short, technology moves quickly and in unexpected ways, often leaving policymakers to play catchup. However, when the nature of the threat carries costs as high as insider threats can, organizational policies and mitigation strategies must remain current.

Early examinations of behavioral insider threats began with wanting to better understand espionage and its motivators. In many instances, espionage is perpetrated by insiders, as most cases of espionage involve those with access to protected knowledge, and thus are insiders by definition (*Insider Threat - Cyber* | CISA, n.d.). That is, when insiders steal information to benefit another organization or country,
they are considered spies (Data Loss Prevention, 2019). Said simply, while not all insiders are spies, most spies are insiders, especially those who fall under the scope of classic espionage, described below.

While PERSEREC—the Defense Personnel and Security Research Center—was created in 1986 in the wake of the John Walker spy ring, the primary espionage statutes (Title 18 U.S.C. § 792-798), passed in 1917, have not changed since 1950 (Herbig, 2017). However, espionage in practice has evolved dramatically since that time. The 1950 statute was written regarding the threat of the time, which, as described above, is generally now considered to be classic espionage. Classic espionage aligns more closely with the notions held by the public—that is, the idea of foreign actors who sneak their way into positions that provide them access to privileged information regarding our government, military, and other protected and secure private institutions.

Like most discussions that touch on acts of relevance to policymakers, we must first discuss what constitutes espionage in the real world. Espionage, in its simplest form, refers to spying. However, there are a range of forms of espionage, many of which diverge from our general conception of a spy infiltrating a protected agency, or classic espionage. A brief history of espionage in the United States helps us understand and distinguish between the various types of espionage, as well as the current state of (and responses to) espionage. This, in turn, informs our understanding of insider threats, as the origin of insider threats as a concept is born out of our efforts to counter and deter espionage efforts against us.

All forms of espionage, as a rule, involve the transfer of secret or protected information to another state entity, which is done covertly. While this typically involves the transfer to another state or other adversarial actors, in recent years, whistleblowers such as Edward Snowden have instead sought to release information to the public about their own government (referred to as “leakage”; CDSE Insider Threat Awareness INT101.16). The various forms of espionage are outlined below.

**Types of Espionage**

There is wide variation in types of espionage as well as an evolution of espionage more generally since the Cold War era. Classic espionage is formally defined as activities done for national government “A,” which acts through an agent who clandestinely collects secrets from national government “B” that wants to control those secrets, and who turns them over to national government “A.” (Herbig, 2017, p. 64). The classic spy also stands out as the “original insider.” That is, those who used deception to infiltrate secure facilities/organizations/personnel to steal information historically did so by becoming insiders (Insider Threat - Cyber | CISA, n.d.). They then abused their access as insiders to obtain secrets. Classic espionage usually involves theft of some sort and generally requires an alternate identity, false flags, or another form of deceit. Definitions of classic espionage include A Context of competition; Political, military, or economic secrets; Theft; Subterfuge and surveillance; Illegality; Psychological toll to the spy.

Classic espionage also covers acting as an agent of a foreign government. The FARA (Foreign Agent Registration Act) of 1938 is the primary way the U.S. federal government tracks these actors. Additionally, there is a parallel statute of the same name and year that primarily serves as the enforcement mechanism for failures to comply with the FARA. Potential offenses include clandestine

---

10 It is worth noting that this statute, as well as preceding statutes that are frequently applied to espionage crimes, do not necessarily require transferred information to be classified.

11 https://www.cdse.edu/Training/eLearning/INT101-signup/

operations, intelligence gathering, illegality, sabotage, terrorism, false identity, and the international proliferation of weapons of mass destruction. There have been increases in both registration and prosecutions over time, suggesting more foreign governments are attempting to spy on the US than in previous years.

However, this “hands-on” method of espionage is shifting toward more leaks and cyber espionage conducted directly by foreign powers. Classic espionage still exists and should not be discounted; however, the nature and mode of espionage have shifted dramatically since the Cold War era corresponding to developments in information technologies and geopolitical relations. In recent years, leaks of classified information have received more attention. Leaks are “disclosures of classified information to the public. They are usually accomplished through the press or by publication in print or electronic media. A leak often follows the form of classic espionage except that the recipient is different” (Herbig, 2017, p. 77). This is largely due to several high-profile leakers over the past decade in the US, such as Edward Snowden and Chelsea Manning. Leakers are generally not subject to whistleblower protections, but public support may vary depending on the nature of the leak. This was demonstrated by mixed public reactions in the fallout of the Snowden leak. For leakers, "An additional controversial element in the debate about leaks is the tension between the need for government secrets and the First Amendment" (Herbig, 2017, p. 77). This also speaks to a need for reform of espionage statutes.

Finally, we must also consider economic espionage, which generally refers to the theft of information by or for a foreign government and is a significant enough loss that it could have implications for the economy of the entire nation. “Industrial” and “corporate” espionage, in contrast, generally refers to theft from one company to another. While industrial and corporate espionage are typically domestic, these thefts may also have far-reaching economic implications. Trade secrets, often the target of corporate espionage, differ from classic espionage in that they don’t involve classified information, but instead focus on the theft of privately owned intellectual property. The US Government has stated that “it will not use the intelligence apparatus of the federal government to conduct economic espionage against other nations for the benefit of American companies” (Herbig, 2017, p. 133). This distinguishes the US Government from other countries that do separate private entities from foreign governments.

The Economic Espionage Act (EEA) of 1996 was passed, in part, due to increases in the storage of information electronically, also how technology and information sharing have shifted our response to and understanding of espionage. Trade secrets don’t have to be sold to foreign governments to qualify under this act—they simply must be going to a “foreign instrumentality,” Further, violations of export control laws can be considered economic espionage if they include the sale, export, or retransfer of various American defense articles and knowledge. This can include military technologies and software, defense services, conventional weapons, missile technology, satellites, and nuclear, chemical, or biological materials and/or weapons (U.S.C. Title 22 - FOREIGN RELATIONS AND INTERCOURSE, 2010). The EEA was passed in 1996, but the underlying language assumes a Cold War context (Herbig, 2017). The dynamics of the global stage have changed significantly since then, with a range of potential nefarious foreign actors. There is general agreement among experts that these statutes need to be updated, but as of this writing, no agreement exists regarding how or in what direction. Ultimately, at its

---

13 https://www.washingtonpost.com/opinions/wassnowden-herooortraitor-perhapsalittleof-both/2017/01/19/a2b8592ec6f011e6bf4b-2c064d32o4bf_story.html

14 Foreign instrumentality: any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government (Definition: Foreign Instrumentality from 18 USC § 1839(1) | LII / Legal Information Institute, 1996)
simplest level, the EEA is designed to protect technology that the US Government owns and does not want exposed.

As implied above, the nature of and trends in espionage have shifted dramatically alongside the increased use of IS&T. And while the advent of IS&T allows for many advantages for potential spies, it also potentially makes their actions more trackable than in previous generations. That is, IS&T follows everyone, including spies and leakers. As one observer noted, “A much bigger worry for spies is that the very vulnerabilities which make it easy for them to steal other people’s secrets also make it hard for them to hold on to their own” (Herbig, 2017, p. 158). This change has also resulted in the advent of cyber espionage by foreign governments. In this way, both the increase of IS&T and globalization stand out as a paradigm shift in the study and understanding of espionage and mass leakers. That is, federal entities like the US now have more adversaries, causing a range of potential entry points rather than one or a handful of nation-state adversaries.

Further changing the security landscape is economic globalization. Increasingly, large corporations operate in multiple countries, creating more opportunities for foreign intervention in those companies. Alternatively, increasing economic globalization has led to the hypothesis of greater cultural globalization. Cultural globalization could, in theory, decrease the risk of espionage due to the alignment of economic interests, but increase the probability of individual violations in support of a “greater good.” This line of thinking has been used, in part, to explain the recent trend of mass leakers who release information for ideological reasons outside of providing information to an adversary or even for financial gain (Thompson, 2018). Alongside a shift like espionage in the context of an increasingly interconnected world, the tempo of mass public disclosures, or mass leaks, appears to be increasing (Gioe & Hatfield, 2021). This is occurring alongside the trend that departs from classic espionage and the Cold War paradigm, where actors are increasingly engaging in espionage activities without any influence from a foreign power or entity. Regardless of motivation, it is undeniable that we are in an increasingly interconnected world, both globally and electronically. As Gioe & Hatfield (2021) note:

“Even without such a verdict, however, the implications of trusted insiders with special system access privileges are profound, revealing the scope of the challenge for intelligence and security communities as well as their oversight bodies. Technology – in the early 21st century – favors the leaker from the inside and the hacker from the outside.” (p. 734).

**Offender Characteristics**

Herbig (2017) recently comprehensively summarized/analyzed decades of research and espionage case analysis on behalf of PERSREC. Three cohorts are compared based on when the individual began espionage: 1947-1979, 1980-1989, and 1990-2015. Most of what we know about the characteristics of spies comes from these cohort studies.

Ultimately, there is no single profile for a spy or mass leaker. We do know some general characteristics, largely based on who has been charged with espionage in the past. Despite financial gains serving as a major motivating factor, those convicted of espionage are almost exclusively middle class (Thompson, 2014). However, we also know that financial motivations rarely stand alone as motivating factors. That is, there are undoubtedly many insiders with potentially highly valued access who do not turn to espionage as a means of financial gain. We also know from previous research that spies often have pathological personality features that may help separate them from their non-spy peers. That is, they are often thrill seekers, frequently exhibit narcissistic tendencies such as grandiosity, and desire power and control (Thompson, 2014; Wilder, 2017). Generally, these personality traits and their unique access can be seen as preconditions for espionage.
Another characteristic is the presence of some sort of critical triggering event that causes acute personal distress (Shaw & Sellers, 2015; Wilder, 2017). Past case analysis illustrates a range of triggering events that precipitated engagement in espionage (Herbig, 2017). This can include a sudden moral qualm, a personal grievance at the workplace, disgruntlement, economic hardship, or personal problems at home. The individual must then not only have access to protected information but also a source willing to receive and reward that information. In the past, this typically referred to a foreign agent responsible for grooming and handling the spy. However, with mass leaking often referred to as “new” espionage, the digital era allows individuals to widely disseminate protected knowledge, such as in the Edward Snowden case. In these cases, a third party is not necessarily involved in either requesting or disseminating protected information. What remains less clear about this shift in behaviors is whether those engaging in mass leaking share different characteristics than those who fit the classic espionage profile. Personality traits associated with espionage include narcissism, psychopathy, and immaturity, while those associated with mass leaking often exhibit grandiosity, and are generally motivated by personal convictions or a concept of the “greater good” (Herbig, 2017; Thompson, 2014, 2018; Wilder, 2017).

The overwhelming majority of those convicted of espionage are middle-class and male (Herbig, 2017). While a majority are white, this has been trending downward over time, with only 55% of the most recent cohort identifying as white. In general, those convicted of espionage are more likely to take risks or have committed crimes, and overall, the education level of spies is increasing over time. That is, individuals recently convicted of espionage have higher average levels of education than those convicted previously. In addition, the average age of those convicted of espionage is increasing. In short, “recent persons convicted of espionage-related offenses have been male, middle-aged, well-educated, and of a variety of racial and ethnic backgrounds that mirrors the increasing level of education and diversity of American society” (Herbig, 2017, p. 12). Another noteworthy trend in convicted spies is the increase in civilian convictions. The proportion of civilian spies increased from about 50% of all convictions to over 75% between two recent PERSEC cohorts, corresponding with increased government contractor hiring in the post-9/11 era—a finding with potentially important policy implications.

Motivational Factors for Engaging in Espionage and Leaking

A prevailing theory of espionage engagement presents the conditions that must occur for a person to engage in espionage: (a) perceived opportunity, (b) contemplation of the act, (c) strong desire to obtain the likely outcomes of engaging in the act, (d) insufficient internal control mechanism, and (e) insufficient external controls. In theory, if one condition is not present, then espionage will not occur in that instance (Timm, 1991). However, this general model fails to adequately describe why an individual desires the outcomes of engaging in the act. The motivations for engaging in espionage generally fall into one of the following categories: economic, ideological, and disgruntlement/revenge. However, when analyzing cases, researchers find that there are often multiple motivations at play. Also, as described above, researchers are increasingly seeing individuals driven by personal beliefs who leak mass information to the public for the sake of fairness or “what’s right.” This is demonstrated by the motivational factors identified among PERSEC’s latest studied cohort of leakers:

- The leakers strongly objected to something they saw being done in the course of their work.
- The leakers enjoyed playing the role of expert.
- The leakers wanted to help and saw themselves as helping.

However, Thompson (2018) argues that mass leakers, along the lines of Snowden and Manning, represent a new type of “spy” altogether that requires their own framework for understanding risk.
factors and motivations. He finds that the intersection of disgruntlement and narcissism are prominent features in mass leaking cases, which aligns with findings in espionage more generally. However, mass leakers are also motivated by a grandiose need for recognition. These motivations, combined with a media infrastructure that encourages a culture of “non-restraint” create the conditions for mass leaking. Similarly, Lillbacka (2017) argues that social context is an important consideration in understanding the motivations of spies and mass leakers. While it is generally regarded that “true” (that is, those motivated by ideology alone) ideologically motivated spies are a minority, ideology is a recurring theme across espionage cases.

Some with protected information have committed espionage due to the promise of extreme wealth or other dramatic returns in exchange for their insider knowledge. Others, like Snowden, claim purely altruistic or ideological purposes. However, these are not mutually exclusive. Rather, they can be seen as working together, alongside the conditions surrounding espionage. That is, if an insider is already disgruntled with their employer and receives an offer of financial gain in exchange for insider knowledge, and provided other necessary conditions are present, deciding to leak or actively spy may be an easier one. Even among ideologically motivated leakers, there are often other motivational factors at play. For example, consider Jonathan Pollard, a U.S. Navy spy who sold state secrets to Israel. Despite receiving financial gains in return for secrets, he contends that his only motivation was to provide information to Israel. Further, he claims information sharing should have been occurring already, therefore he was “righting” an existing “wrong.” While ideological motivations were likely a component of his espionage activities, the reality is that Pollard also received financial benefits in exchange for secrets, and ideology is unlikely to stand alone as a motivator.

**Sabotage**

In addition to espionage, insider threat scholars and practitioners have classified sabotage as a major category of malicious insider behavior (Giacalone & Promislo, 2010; Greitzer et al., 2010; Kont et al., 2015; Theis et al., 2019). Whereas espionage entails gathering useful information to further the interests of parties outside the organization, the primary goal of sabotage is to interfere with and harm the processes and behaviors of those inside the organization (Giacalone & Promislo, 2010). Accordingly, sabotage involves intentionally impeding an organization’s valued goals by withholding, tampering with, or destroying critical resources (e.g., information, tools, labor) that organization members rely on for their work (Analoui, 1995; Crino, 1994). The harm done by acts of sabotage generally occurs through process losses instead of direct psychological or physical damage (e.g., verbal aggression, workplace violence), but the form of sabotage varies based on the context, abilities, and motivations of deviant insiders (Ambrose, 2002; Greitzer et al., 2010; Liu et al., 2022; Schwepker Jr. & Dimitriou, 2022).

Research on organizational sabotage spans multiple disciplines including organizational behavior, hospitality management, risk and threat assessment, management information systems, and cybersecurity. Across these domains, scholars have examined four main classes of sabotage behaviors: production, service, knowledge, and IS&T. The many forms of sabotage represent insider threats to different organizational resources, vulnerabilities, and processes, and as such, pose distinct implications for prevention, detection, mitigation, and harm. Protecting organizational assets from sabotage thus requires a baseline understanding of the sources and types of sabotage behavior.

**PRODUCTION SABOTAGE**

Production sabotage refers to the deliberate slowing or halting of an organization’s production processes (Hollinger & Clark, 1982). This type of sabotage tends to occur in work environments where employees’ activities are interdependent (often sequential) and combine to yield material end-products (Saavedra et al., 1993; Taylor & Walton, 1971), such as assembly line manufacturing or R&D. Milder
cases of production sabotage include production-slowing behaviors such as effort withholding, defying orders, or quitting. At more extreme levels, employees can disable production entirely through supply chain blockage, strikes, or destruction of machinery (Brown, 1977; Giacalone & Rosenfeld, 1987). Cases of production sabotage can cause substantial damage to an organization’s tangible and intangible assets.

SERVICE SABOTAGE
Service sabotage involves behaviors of employees that are intended to undermine customer service and interests (Cheng et al., 2020). This form of sabotage can occur in any customer-facing role in the service and hospitality industries. Examples of service sabotage include verbal hostility toward customers, delaying service, tampering with customer product orders, and deliberately failing to meet customer service requests (Harris & Ogbonna, 2006). The intentional interruption of customer service typically occurs at the direct expense of the customer, with indirect financial and reputational losses to the employer (Kao & Cheng, 2017; Liu et al., 2022).

KNOWLEDGE SABOTAGE
Knowledge sabotage occurs when employees hide key workrelated information or share false (i.e., misrepresented or fabricated) knowledge to mislead fellow workers and impede their ability to execute work tasks (Serenko, 2020). Much like service sabotage, knowledge sabotage occurs through interpersonal exchanges, but these behaviors differ in that knowledge sabotage targets co-workers more so than customers. Further, knowledge sabotage is distinct from benign cases of knowledge tampering such as white lies or unintentional knowledge hoarding, as the central aim of knowledge sabotage is to harm worker effectiveness and work processes (Connelly et al., 2012; Ferraris & Perotti, 2020). The severity of knowledge sabotage corresponds directly with the necessity of information for work-related processes and its exclusivity (i.e., the more critical and inaccessible the information is, the more harmful it is for one to withhold it).

IT SABOTAGE
IT sabotage is broadly defined as an insider’s malicious abuse of privileged IT system access to cause harm to an organization and its members (Band et al., 2006; Greitzer, 2019). This can entail altering, hiding, or deleting important files (manually, or via an installation of bugs and other rogue devices); fabricating information that mocks or damages the reputation of an organization; or disabling employees’ access to electronic information, networks, or systems that are vital to conducting their work (Cappelli et al., 2012; Keeney et al., 2005). The outcomes of IT sabotage can range from operational impediments (e.g., halting of work and work processes, loss of time, increased employee workload) to reputational impairment (e.g., unfavorable perceptions from customers, distributors, suppliers, or other stakeholders) and financial loss (e.g., reduced production, loss of clientele, the monetary cost of repairing damages). Additionally, IT sabotage can coincide with other forms of sabotage, as production machinery, personnel management software, customer support processes, and organizational data storage tend to be housed within IT systems.

Insider Motivations for Sabotage
Motivations for sabotage typically originate from self-interest and/or animosity toward an organization and its people (Serenko, 2020). More specifically, people enact sabotage behaviors when they seek to gain a competitive advantage over others at work or seek revenge for interpersonal or organizational grievances (Choo & Serenko, 2020; Crino, 1994; Gruys & Sackett, 2003). Hiding valuable information from coworkers, for example, gives individuals near-exclusive access to necessary work-related information and places them in a position of relative power to others who must then rely on the knowledge holders (i.e., brokers) for information (Kwon et al., 2020; Perotti et al., 2022). Situations that
fuel retaliatory acts of sabotage may include customer mistreatment (Liu et al., 2022; Scarlicki et al., 2008), interpersonal conflict at work (Eissa & Wyland, 2016), and frustration or ethical conflict with one’s work and organization (Ambrose et al., 2002; Chen et al., 1992; Kont et al., 2015; Schwepker Jr. & Dimitriou, 2022). Taken together, most insider sabotage events generally arise from self-gratification or retribution motives, but the nature of actions taken hinges on the insider’s access to critical organizational resources and capacity to thwart organizational processes.

**Workplace Violence**

Given high-profile cases of kinetic violence, such as Nidal Hasan’s terrorist attack on the Fort Hood installation, insider threat researchers have a significant interest in reducing risks from such violence in their workplace. However, in examining workplace violence scholarship and practice, definitional issues emerge in mapping that literature onto counter-insider threat research and practice. Specifically, researchers often distinguish between workplace aggression and workplace violence. Geck and colleagues (2017) define aggression as, “deliberate behavior by an employee who intended to or actually harmed another employee, with the emphasis being on psychological harm and not physical harm,” and violence as, “workplace behavior that either inflicted physical harm or intended to inflict physical harm on another employee” (p. 211). Thus, the workplace violence literature uses a broader definition of violence than is frequently considered by insider threat researchers.

Scholars who study workplace violence further distinguish among four types of workplace violence that vary by the relationship between the perpetrator and the organization (e.g., CDC, 2004; CISA, 2019; and Geck et al., 2017):

- **Criminal Intent.** In this type of workplace violence, the perpetrator has no legitimate relationship with the organization and is perpetuating violence as part of a criminal motive, such as robbery.
- **Customer.** In this type of workplace violence, the perpetrator is a client, customer, student, or other similar status. Thus, the perpetrator has a legitimate relationship with the organization but is not considered part of the organization.
- **Employee.** This type of workplace violence is perpetrated by a current or former employee and would typically be considered an “insider threat.”
- **Personal Relationship.** In this type of workplace violence, the perpetrator has a relationship or association with someone in the organization, but not the organization itself. Often these are domestic disputes that carry over to the workplace context.

Workplace violence is rare and driven by occupational settings such that the first two types of workplace violence are most likely to occur in organizations that interface regularly with the public (Piquero et al., 2013). The Bureau of Justice Statistics (BJS), aggregating multiple nationally representative data sources, found the rate of nonfatal workplace violence to be 9.2 violent crimes per 1,000 workers (age 16 or older), with higher rates being observed in specific occupations such as mental health professionals (46.1 per 1,000), law enforcement officers (82.9 per 1,000), corrections officers (146.1 per 1,000), and bartenders (70.9 per 1,000) (Harrell et al., 2022; though it is widely agreed that workplace violence is underreported, see CDC, 2004). Because the incidence of workplace violence is skewed towards certain occupations, much of the literature focuses on risk factors and mitigation in certain domains (e.g., health care). Empirical literature specifically examining workerto-worker workplace violence is rare, as it is far less prevalent than criminal and customer violence (Piquero et al., 2013). We summarize the relevant literature that is available next.
Workplace Violence Risk Factors

Given the wide variation by job, research and practice guides on identifying risk factors for workplace violence tend to focus on job and organizational characteristics. LeBlanc and Kelloway (2002) developed a job characteristics survey and found 22 items to be correlated with self-reported incidence of violence. These factors included job responsibilities (e.g., physical care of others, handling guns), context (e.g., working alone during the day), and customers (e.g., contact with individuals under the influence of alcohol). The Occupational Health and Safety Administration (OSHA, 2016), in their recommendations for the healthcare and social service sectors, identified additional risk factors associated with the organization or work setting, such as lack of staff training (lack of experience also comes up regularly as a risk factor in a review by Piquero et al., 2013), understaffing, high turnover, inadequate security, poor space design, and poor organizational processes. The Society for Human Resource Management (SHRM, 2023) also identifies “risky situations” in the workplace that may increase the risk of violence, including terminations and working with individuals with mental illness. Other problematic organizational responses (e.g., not taking indicators of risk seriously) are also likely to increase the probability of workplace violence or other negative outcomes (Lenzenweger & Shaw, 2022; Shaw & Sellars, 2015).

Geck and colleagues (2017) performed one of the few empirical studies examining individual risk factors for aggression and violence in a workplace setting. Building off an established set of eight risk factors associated with interpersonal violence,15 the authors examined referrals to a workplace violence clinic and content-coded the case files. In comparing violent to aggressive cases, they found that violent individuals were (a) more likely to have a marital status, potentially suggesting a spillover effect from home, (b) less likely to have been diagnosed with a mental illness, (c) less likely to have a history of threats, but more likely to have a history of violence in the workplace. In comparing one-time violent employees to those who were violent more than once, they found repeaters were more likely to have experienced physical abuse early in life, have a mental health diagnosis, and have workplace histories of concerning behavior. Viñas-Racionero, Scalora, and Cawood (2021) used items from two Structured Professional Judgment (SPJ) to review 40 scenarios where individuals were exhibiting behaviors of concern. They found five indicators to be correlated at a statistically significant level with violent outcomes: (a) motives for violence, (b) homicidal fantasies/violent preoccupations, (c) weapon skill/access/involvement, (d) preattack planning and preparation, and (e) suicidality/depression.

Other practitioner-focused resources emphasize proximal indicators of potential violence. For example, CISA provides a brochure of indicators for employers to be on the lookout for, such as “increasingly erratic, unsafe, or aggressive behaviors” and “sudden and dramatic changes in home life or personality” (CISA, 2019; see Figure 4 for the full brochure and SHRM, 2023; OSHA, 2016 for additional examples).

These indicators are consistent with some of the “concerning behaviors” described in the critical pathway model referenced previously (Lenzenweger & Shaw, 2022; Shaw & Sellars, 2015) as well as SPJ tools focused on workplace violence, such as the Workplace Assessment of Violence Risk (WAVR-21; White, 2021).

---

As it relates to insider threat, the practice guides referenced above tend to focus on two types of mitigation strategies: (a) removing barriers to workplace violence prevention strategies and (b) specific strategies for reducing the probability of worker-on-worker violence. Concerning the former, CDC (2004), for example, suggests organizations take workplace violence seriously by investing resources and committing to process improvements. Some suggestions for accomplishing these goals include, for example (CDC, 2004; CISA, 2019; OSHA, 2016), ensuring management and worker commitment; having a written workplace violence policy; establishing workplace violence prevention programs that include a wide range of stakeholders (e.g., security, HR, legal, management); providing appropriate training to employees; and regularly reviewing, evaluating, and improving upon those programs. Concerning preventing worker-on-worker violence specifically, CISA (2019) provides the most comprehensive set of recommendations based on our review. While written to support workplace violence prevention efforts within the federal government, many of the recommendations generalize to other large organizations, including establishing:

---

• Screening processes to select individuals at an elevated risk of committing violence. This includes implementing pre-employment vetting processes (e.g., reference checks) and making use of probationary periods.
• Training programs to protect the workforce from potential violence. This includes training for employees (e.g., on policies and procedures, as well as prevention strategies, such as anger and stress management), supervisors, and incident response teams.
• Alternative Dispute Resolution (ADR) programs. ADR is an umbrella term for resolving disagreements through a neutral third party, such as ombudsmen, facilitation, and mediation.
• Incident response or threat assessment teams. Summarizing current best practices for workplace threat assessment teams specifically is beyond the scope of the current section but is a critical element in workplace violence prevention.
• Employee Assistance Programs (EAPs). EAPs can be critical to early intervention efforts.
• Processes to help organizations recover after an incident. This involves the identification of trained mental health professionals and the deployment of procedures (e.g., the Psychological First Aid model) to assist with recovery.

Social and Behavioral Science Perspectives
While the previous section described practitioner-focused perspectives, the next four subsections describe academic literature, at a high level, related to insider threat. Two of the sections – political violence and counterproductive work behaviors – provide foundational theoretical information and data that enhance how we understand insider threats. Specifically, the political violence literature addresses a gap identified in Part 1—the role that groups and/or ideology may play in insider threats. The literature on counterproductive work behaviors helps to enhance our understanding of potential antecedents and contextual factors that predict the maladaptive behaviors thought to be indicative of insider threat. The other two sections – preventing terrorism/targeted violence and adaptability – provide information that can be used in developing insider threat mitigation strategies. As the name implies, research into preventing terrorism and targeted violence examines community-based mitigation strategies for ideologically and non-ideologically motivated violence. We examine this literature to see if lessons may be learned for countering insider threats. Following the general finding from Part 1 that disgruntled employees are far more likely to become insider threats, the adaptability literature provides a potential theoretical framework for avoiding negative employee outcomes (and enhancing positive outcomes) that increase insider threat risk.

Political Violence
With ideologically motivated insider threats, we turn to lessons from political violence to better understand the reasoning behind, for example, leaks and intellectual property thefts. Many convicted spies explain that perceive immorality or that they are engaging as a form of revenge against an agency (Thompson, 2018). Insiders pose a unique challenge for security professionals. They are uniquely positioned to cause more significant harm than average civilians who do not already have access to protected spaces and information. The distinction comes from their position within an organization, rather than any particular traits that are otherwise unique to other forms of criminals. In this sense, we can take the lessons learned from the targeted violence and political violence space. This area of research has sought to understand domestic violent extremism, whose attributes parallel those of insider threat. Although discussions about what constitutes domestic violent extremism (DVE) are contentious and nuanced in academic circles (Bennett & Lewis, 2022; Hoffman, 2017), we use it broadly here in reference to violent extremism and targeted violence between perpetrators and victims with the same citizenship. In its most basic sense, violent extremism refers to violence that occurs in the name of an
extremist ideology, whereas targeted violence refers to acts of violence that are preplanned and intentional – that is, that have a target in mind – but that are not motivated by political, ideological, or religious goals (McBride et al., 2021).

Recently, violent extremism and targeted violence have been formally recognized as internal threats to national security, prompting the United States government to release its firstever National Strategy for Countering Domestic Terrorism (U.S. National Security Council, 2021). The current domestic violent extremist threat is further classified into two main threads: Anti-government or Anti-authority Violent Extremists (AGAAVE) and Racially and Ethnically Motivated Violent Extremism (REMVE). While there is substantive overlap, the former predominately targets institutions and other symbols of institutional authority (i.e., the Federal Government, police officers), whereas the latter focuses on violence targeted against individuals (i.e., members of a particular racial or ethnic group). These distinctions are intended to separate the motives behind violent acts, but the reality is that radical beliefs alone are not sufficient motives for violence (Asal et al., 2017; McCauley & Moskalenko, 2017; Wolfowicz et al., 2021). That is, radical beliefs alone are not a “conveyor belt” that leads ultimately to violent extremism. They may, however, be suggestive of how or at whom violence will be used, and when they exist alongside other risk factors, the likelihood of violence may increase.

Researchers are still working to understand what distinguishes those who engage in violence from other, nonviolent ideological extremists. However, what is increasingly clear is that it is not static factors that best predict the risk of violence, but rather, dynamic ones. For example, fixed traits such as race, nationality, age, and sex are generally poor predictors of violence, regardless of an individual’s level of extremism. Instead, the sociopolitical environments in which people are embedded, and their interactions with those environments, better serve to conceptualize domestic violence risk (Neo et al., 2017). For instance, while REMVE attackers have accounted for the majority of recent DVE attacks in the United States, AGAAVE attackers pose a greater risk to law enforcement and other authority figures resulting from situational interactions such as traffic stops (Clifford, 2021; “Strategic Intelligence Assessment and Data on Domestic Terrorism, 2021).” 2021).

Such differences between these violent extremists suggest that discrete triggering events or contexts, in combination with one’s beliefs, can increase the perceived viability and likelihood of violent behavior (Hamm & Spaaij, 2015). This parallels significantly with lessons from espionage, in that a triggering event aligns with opportunity and individual personality pathologies such as thrill-seeking behavior for an act of espionage to occur. Additionally, group norms and group membership can convince those with grievances and aggressive tendencies (or even those without, who join groups and movements out of social pressure or solidarity) to justify their mobilization toward violence for social and political aims (Asal et al., 2017; Clifford & Lewis, 2022). Thus, although radical beliefs are of concern, the foundations of violent actions are often also social or contextual.

With that said, it is also worth noting that the dynamics around foreign actors and their role in espionage have evolved alongside technology. That is, after the Cold War, the dynamic began to shift to a threat of multiple state actors of ranging power, as opposed to one major superpower. In addition, actors working outside of the behest of a nation began to emerge. The increased reliance on IS&T has contributed to this shift by enabling outsiders access without needing to physically infiltrate a facility, such as in the case of cyberhackers who leak. While many hackers breach protected information to sell personal data for profit, others are ideologically motivated, and the two often intertwine. Take, for example, the hacktivist group Anonymous. Most recently, Anonymous has been in the news for

17 Hacktivism: Hacking to achieve social action or political objectives.
attacking Russian computer systems in protest of the 2022 Russian Invasion of Ukraine (*Russia-Ukraine War*, n.d.). However, Anonymous is not Ukrainian. Anonymous has no national identity, other than as a global collective that transcends global borders. Therefore, cyberattacks against the Russian state are in favor of one nation, but not acting on behalf of that nation. In addition, this is one of dozens of causes Anonymous has been involved in since its inception.

This is further demonstrated by massive leaking cases over the past decade committed by individuals with no allegiance to a particular nation or even, an extremist ideology. Consider the case of Edward Snowden. He leaked highly classified information as an American citizen while working for the National Security Agency (NSA) as a subcontractor. He was in no way working as a foreign actor or at the behest of an ideological group or even mission; rather, while working at the NSA, he claims that he became increasingly disillusioned and that his formal disputes were ignored (*Snowden Speaks: A Vanity Fair Special Report* | *Vanity Fair*, n.d.). Cases like Snowden and Anonymous underly the shifting nature of both technology and an increasingly globalized world, as well as how they impact espionage and insider threats.

**Terrorism and Targeted Violence Prevention**

Recognizing ideologically motivated threats such as those described in the previous section, governments around the globe began in the early 2010s developing programs to counter terrorism from domestic sources. These programs, commonly known as “countering violent extremism” (CVE) programs in the academic literature, have several lines of effort and best practices associated with them (Stephens et al., 2021; NCITE, 2022b). In 2019, DHS published the *Strategic Framework for Countering Terrorism and Targeted Violence* that added targeted violence to domestic security concerns. The core difference between terrorism and targeted violence is perpetrators in the latter category lack “a clearly discernible political, ideological, or religious motivation,” but both “are of such severity and magnitude as to suggest an intent to inflict a degree of mass injury, destruction, or death” (DHS, 2019; p. 4). Terrorism and targeted violence prevention then is a catch-all term for a wide variety of programming thought to prevent violence through non-criminal-justice-oriented means, such as programs to increase resilience (in both individuals and communities), countering narratives, disengagement programming, rehabilitation and reintegration, and so forth (Jackson et al., 2019; Sinai et al., 2019). Further, given the recency of these programs, challenges in community-based data collection, and the diversity of programming, there is a lack of empirical evidence to test targeted violence and terrorism prevention programs and associated underlying models (NCITE, 2022b; Sinai et al., 2019; Mastroe & Szmania, 2016). Despite these limitations, we believe there is still value in surveying the state of this literature to determine whether any insights can be gleaned into insider threat research and practice.

With respect to theory, underlying CVE/counterterrorism programming is a “critical pathway”-type model that identifies vulnerable populations who start to become radicalized and eventually mobilize to violence. The RAND Corporation (Jackson et al., 2019), in a detailed review of the extant literature and interviews with subject matter experts of all types, developed the process model presented in Figure 4, which represents this underlying theory and maps DHS programming onto it. One can see many similarities with Figure 3 presented previously, suggesting lessons learned in one field could potentially inform another. Concerning targeted violence, there is no one underlying theoretical model. McBride and colleagues (2022) present five potential underlying theoretical models, but synthesis is needed as theories often diverge greatly in their explanations of targeted violence. For example, the “Developmental Pathways to Demonstrative Targeted Attacks” theory suggests that perpetrators all follow a very similar pathway to targeted violence, while the “Intimate Massacres Model” theory suggests multiple pathways to violence.
Figure 5. Radicalization and Terrorism Prevention Framework (Jackson et al., 2019)

Although these programs are still relatively new, enough work has been done around the world in the last 10+ years that summary reviews of available evidence have led to convergence on a few best practices that may find relevance to counterinsider threat programming. We should also note that there is a lot of programming that is irrelevant to the insider threat context. To take an obvious example, recidivism reduction programs would not be in the purview of an individual organization. However, there are some transferrable lessons, the most relevant of which we describe below:

- **Countering terrorism and targeted violence programs should be community-based.** A consistent recommendation among scholars in this space is that programming should be (a) community-driven, where community leaders identify programming needs, and (b) highly customized to the needs of each community (Sinai et al., 2019, Jackson et al., 2019). It is an open question whether counter-insider threat programs should be similarly customized to organizations, a question we will explore in greater detail later in this paper.

- **Emphasize community resilience.** Early CVE programming often focused on identifying communities “at risk” for terrorism and developing programming geared toward a priori steering individuals away from violence. This led to feelings of marginalization by some community members and negative reactions (Jackson et al., 2019; Panduranga, 2021; Schanzer & Eyerman, 2019). This is similar to the backlash effects that can be found with heavy-handed security reactions to behaviors of concern in an insider threat context (e.g., Moore et al., 2015; Shaw & Sellars, 2015). Programs that emphasize community resilience have the advantage of taking a strength versus a deficit-oriented perspective, which is more likely to be positively received, less prejudiced, and easier to evaluate (Stephens et al., 2021).

- **Emphasize coordination and communication within communities.** Another aspect of resilience-focused programming is the need for real partnerships to develop between community
organizations and government entities (Stephens et al., 2021). Having disparate groups work together from different perspectives on a common goal can be powerful. Additionally, effective targeted violence and terrorism prevention programs draw upon a wide range of disciplines, such as criminology, education, public health, and psychology (NCITE, 2022b; Stephens et al., 2021). All of this suggests that counter-insider threat should be a team sport, incorporating a variety of groups and disciplines that may include groups such as security, IT, HR, management, unions, and so forth.

- **Build in program evaluation.** Given the newness of targeted violence and terrorism prevention programming, empirical evidence of the effectiveness of different programs is limited. Researchers have called for building evaluation into all programming to contribute to general knowledge regarding what works and does not (NCITE, 2022b). Similarly, organizations should also measure the return on investment in counter-insider threat programming. Programs that focus on resilience (which we describe as adaptability in the section below) are more likely to have positive benefits that go beyond security-oriented needs.

**Workplace deviance and counterproductive work behaviors**
Organizational research on counterproductive work behaviors provides a direct picture of the individual, social, and contextual risk factors for harmful insider behaviors (INSA, 2017). Whereas political violence and preventing terrorism/targeted violence perspectives focus on extreme, outlier attitudes, intentions, and behaviors related to physical violence (Wolffowitz et al., 2021), scientific work on counterproductive work behaviors largely pertains to ordinary employees and their everyday discretionary, nonviolent activity (cf. LeBlanc & Kelloway, 2002; Neuman & Baron, 1998). In other words, harmful behaviors in organizations can unfold without extremist ideologies, radical intentions, or any interpersonal violence. Moreover, in comparison to political violence researchers, organization scholars emphasize the immediate social and organizational context more so than biographical data and life experiences (Gill et al., 2017; Simi et al., 2016). Harmful employee behaviors, through this perspective, are a product not only of individuals, but their interactions with others and reactions to organizational policies, practices, and procedures (Mackey et al., 2021). We provide a broad overview of this research area by describing the actions that fall within the umbrella of counterproductive work behaviors (and the targets of such behaviors), their common correlates, and implications for insider risk and threat assessment.

Counterproductive work behaviors are defined as voluntary employee behaviors that reduce worker effectiveness and harm the organization’s property, personnel, or functioning (Bennett et al., 2018). The definition of counterproductive workplace behaviors is similar to that of workplace deviance (i.e., voluntary employee behavior that violates organizational norms and harms the organization and its constituents), such that the terms are frequently used interchangeably (Carpenter & Berry, 2017). Although the differences are negligible, some researchers view workplace deviance as a subset of counterproductive behaviors that more explicitly violate norms (Mackey et al., 2021) because not all counterproductive work behaviors are non-normative (e.g., conflict with coworkers or withdrawal behaviors). For simplicity, however, we will use the broader term of counterproductive work behaviors.

**Models of Counterproductive Work Behavior**
Three main empirical models catalogue the structure of counterproductive work behaviors. Within these models, researchers primarily conceptualize counterproductive work behaviors by the content or target of behaviors (Marcus et al., 2016). Content refers to the types of specific work-related activities that fit within the definition of counterproductive work behaviors, and these behavior categories vary in their severity or potential for harm. In addition to behavior types, researchers also specify to whom or what such behaviors are targeted. These three models of counterproductive work behaviors are similar, yet
distinct, as they differ in the extent to which behavioral content and targets are represented. Below, we review the three models briefly and note their similarities and differences.

Bennett and Robinson (2000) provided one of the first measures of counterproductive work behaviors, based on their original conceptual typology of workplace deviance (Robinson & Bennett, 1995). This measure distinguishes between harmful behaviors targeted at individuals within the organization and actions targeted at the organization. The interpersonally oriented behaviors include forms of workplace aggression (Hershcovis, 2011), such as making racially insensitive remarks, cursing at someone, or publicly ridiculing someone at work. Behaviors that harm the organization include but are not limited to theft (of money, physical items, or time), disobedience, littering, on-the-job drug use, and lateness.

Gruys and Sackett (2003) developed what Marcus and colleagues (2016) described as the most comprehensive measure of counterproductive work behaviors. This measure organizes harmful behaviors by their content, which captures 11 behavior categories: (1) theft and theft-related behavior, (2) destruction of property, (3) misuse of information, (4) misuse of time and resources, (5) unsafe behavior, (6) poor attendance, (7) poor quality work, (8) alcohol use, (9) drug use, (10) inappropriate verbal actions, and (11) inappropriate physical actions. In contrast to Bennett and Robinson’s (2000) measure, the behavior content categories capture a broader collection of workplace behaviors that encompass physical actions and harm. The measure by Gruys and Sackett (2003) does not explicitly group items by target, although it does distinguish interpersonally and organizationally directed behaviors.

Spector and colleagues (2006) created a fivefacet model of counterproductive work behaviors that includes abuse, production deviance, sabotage, theft, and withdrawal. Much like Gruys and Sackett (2003), the researchers organized their items based on content rather than targets. However, their model development approach differed from Gruys and Sackett (2003) and Bennett and Robinson (2000) in that they used a theory-driven, rather than a factor-analytic, approach to developing their facets (Marcus et al., 2016). Similar to Bennett and Robinson (2000), the measure represents a narrower coverage of the counterproductive workplace behavior domain in comparison to Gruys and Sackett (2003). The model by Spector et al. (2006) can also be divided into interpersonally and organizationally directed behaviors, but most of their behavior content groupings target the organization, except for abuse. Additionally, a distinguishing feature of this measure is that it excludes items related to substance abuse (argued by some scholars to be selfdirected rather than organizationally directed behaviors; Marcus et al., 2016), which are present in the other two measurement models.

Despite the noted differences in facet structures and comprehensiveness, the behaviors represented within these three counterproductive workplace behavior models can generally be described via their content and targets. These models offer much direct utility to social scientific perspectives on insider threat. In particular, the content and targets of counterproductive work behaviors are crucial considerations for both research and practice because they give insight into how insider activities can manifest to harm an organization and its constituents. Modeling the content and structure of such behaviors, in other words, helps to identify potential behavioral indicators that predict insider threat. Although counterproductive work behaviors have been included in insider threat prediction and detection models (e.g., Bedford & van der Laan, 2021; Greitzer et al., 2018), research has also begun to recognize the importance of more distal antecedents of insider threat (Lenzenweger & Shaw, 2022), which are well-studied in the counterproductive work behavior literature. In fact, research on counterproductive work behaviors extends far beyond descriptive, definitional work and has examined a wealth of predictors such as personality traits, work stressors, attitudes, so–organizational factors, and their interactions (e.g., Berry et al., 2007; Liao et al., 2021; Mackey et al., 2021). Advancing current
insider threat risk models and assessment frameworks thus requires a deeper understanding of common
antecedents of counterproductive work behaviors.

**Correlates of Counterproductive work behaviors**
A large body of research and meta-analyses on counterproductive work behaviors offer ample evidence
for individual, social, and organizational factors that predict, or contribute to, employees’ decisions to
engage in detrimental workplace behaviors. Notably, research evidence indicates that personal and
contextual factors can influence counterproductive work behaviors uniquely by themselves or jointly, in
interaction with each other. Furthermore, different theories have been used to explain the occurrence of
counterproductive work behaviors depending on the nature of the predictors. Here, we summarize the
common correlates of counterproductive work behaviors and the theories that accompany them.

**INDIVIDUAL FACTORS.**
Individual worker characteristics that predict counterproductive work behaviors are mostly dispositional
but also include biographical data. In general, the strongest individual-level correlates of
counterproductive work behaviors include personality traits reflective of less care about an organization,
its work, and its people. Those with low agreeableness, conscientiousness, and emotional intelligence
exhibit more counterproductive work behaviors (e.g., Bowling et al., 2011; Mackey et al., 2021; Zhou et
al., 2014), as do people who score higher on measures of aggression (e.g., Galić & Ružočić, 2017;
Kranefeld & Blickle, 2022; Ružočić et al., 2021; Runge et al., 2020) and Dark Triadic traits (i.e.,
psychopathy, Machiavellianism, narcissism; e.g., Ellen III et al., 2021; O’Boyle et al., 2012). More
specifically, two recent meta-analyses found that conscientiousness (a task- and achievement-focused
trait) was more strongly linked to counterproductive behaviors targeted toward the organization,
whereas agreeableness (i.e., a socially oriented trait) was more strongly related to interpersonal
aggression (e.g., Ellen III et al., 2021; Mackey et al., 2021). Moreover, a metaanalysis by Ellen III et al.
(2021) determined that psychopathy and Machiavellianism were the strongest dark personality links to
counterproductive work behaviors. Demographic variables are generally poor predictors of
counterproductive work behaviors, but there is some evidence that biographical data such as history of
aggression predicts aggressive interpersonal behaviors at work (Douglas & Martinic, 2001; Greenberg
& Barling, 1999; Inness et al., 2005). Together, the individual-level predictors of counterproductive work
behaviors are best explained by models of personality (e.g., Big Five, Dark Triad) and theories of
aggression (Neuman & Baron, 1997), with stronger relationships between traits that match the nature of
the target (e.g., conscientiousness is more strongly linked to carelessness at work and absenteeism
than agreeableness).

**SOCIAL FACTORS.**
Extending beyond individual characteristics, counterproductive work behaviors can also arise from social
experiences, such as deviant peers, experienced incivility, or the relationship between perpetrators and
victims. Social explanations for counterproductive work behaviors are often rooted in social information
processing or exchange theories (Bandura & Walters, 1977; Blau, 1964; Cropanzano & Mitchell, 2005;
Salancik & Pfeffer, 1978). Through social learning and information processing, employees may feel
pressure to model their deviant peers’ behaviors at work (e.g., Azeem et al., 2021; Ferguson & Barry,
2011; Reynolds Kueny et al., 2020; Sakurai & Jex, 2012). In addition to social learning and pressures,
counterproductive work behaviors can stem from anger and frustration that expected social exchanges
at work are not met. Making rude remarks to a coworker, for example, may compel that coworker to
retaliate or even pay that behavior forward to others (e.g., Hauge et al., 2009). Notably, these social
exchanges are not limited to interpersonal conflict. In leader-follower relations, organizationally deviant
follower behaviors (e.g., withdrawal, theft, poor job performance) can lead to interpersonally abusive
supervision (e.g., yelling, belittling, undermining) and vice versa (e.g., Lian et al., 2014; Penney & Spector, 2005; Tepper et al., 2008; Wei & Si, 2013).

**WORKRELATED FACTORS.**

Frustration from one’s work or organizational practices, policies, and procedures can also motivate counterproductive work behaviors (INSA, 2017). Work and organization-related correlates of counterproductive work behaviors usually involve issues of job strain and organizational justice, and they primarily result in harm toward the organization rather than its people. Work conditions that hinder, interfere with, or fail to support employees’ accomplishment of work tasks tend to produce occupational stress and feelings of burnout (e.g., Fox et al., 2001; Meier & Spector, 2013; Penney & Spector, 2005). The resulting strain and job dissatisfaction from work-related constraints can lead employees to engage in counterproductive activity as a coping response, which can range from emotion-focused withdrawal (with little intent to change one’s work conditions) to active resistance (Krischer et al., 2010; Shoss et al., 2016; Peter & O’Connor, 1980; Pindek & Spector, 2016). Similar effects have also been found for job insecurity and person-organization fit (Harold et al., 2016; Mackey et al., 2021). That is, job insecurity and perceptions of poor person-organization fit have been linked to increased expression of counterproductive work behaviors. Further, metaanalytic findings suggest that employees tend to respond adversely to perceived injustices at work, such as unfair pay, lack of informational transparency, inequitable procedures, and psychological contract breaches (Berry et al., 2007; Liao et al., 2021; Mackey et al., 2021). Employees who view their assigned work tasks as illegitimate or above their pay grade, for example, may refuse to do their work at all (Zhao et al., 2022).

**PERSON × SITUATION INTERACTIONS.**

Although the individual, social, and work-related correlates of counterproductive behaviors do exhibit unique effects, organization scholars also recognize that such behaviors are influenced by a mixture of factors. That is, harmful insider behaviors are sometimes more likely to occur when personality traits interact with social and work-related factors. The effects of conscientiousness, agreeableness, and negative affectivity on counterproductive work behaviors, for instance, can be bolstered by negative work perceptions, ambiguity, and unfavorable interpersonal treatment (e.g., Colbert et al., 2004; Yang & Diefendorff, 2009). There is no shortage of potential person-by-situation interactions. What is crucial to note, though, is that situational factors can mitigate or exacerbate the effects of individual predictors. Since personality traits tend to have high stability, it is valuable to understand the influence of controllable, contextual factors (e.g., job characteristics, pay equity) that can be molded to subvert the risk of insider threat events.

**Organizational Adaptability**

In the inaugural issue of the journal *Counter Insider Threat: Research and Practice*, Moore, Gardner, and Rousseau (2022), following research conducted at SEI CERT (Moore et al., 2016), argue that insider threat mitigation programs can be augmented through positive deterrence strategies. Positive deterrence is defined in this paper as “workforce management practices that positively influence the organizational factors and result in reduced insider risk.” They contrast positive deterrence with the “command-and-control” tactics (e.g., security controls) typically relied upon for insider threat risk mitigation. Moore and colleagues further propose that heavy-handed command-and-control tactics may increase the probability of a threat event, suggesting there may be a limit to the amount of command-and-control procedures that an organization can implement before returns to security are diminished or even reversed. Indeed, scholars and practitioners have begun to recognize the importance of the “human dimension” in the context of security generally, and insider threats specifically (e.g., Greitzer,
2019; see also INSA, 2020 and CISA’s publication “HR’s Role in Preventing Insider Threats”\(^{18}\). As one illustration, Hobbs and Moran (2022), in their examination of nuclear security system failures, illustrate that poor individual habits and workplace processes can neutralize even the best command-and-control security systems. As another example, studies have established the relationship between close antecedents to violence, such as workplace aggression, and poor leadership (Alhasnawi & Abbas, 2021; Hepworth & Towler, 2004).

In this section, following Dorsey, Allen, and Ingerick (2020), we propose that research on organizational adaptability may provide an underlying theoretical rationale identifying tools and techniques for (a) enhancing positive deterrence and (b) reacting swiftly and constructively to threat events. Specifically, organizational adaptability research may provide a mechanism for developing policies that act on factors considered to positively deter threat events. Organizational adaptability involves the study of how individuals and organizations respond to changing circumstances (see Baard et al., 2014 for a review).\(^{19}\) Although there are many definitions, scholars generally agree that adaptability (a) has both proactive and reactive components (Griffen et al., 2007; Huang et al., 2014), (b) is context-dependent (Pulakos et al., 2000), and (c) is a “multi-level” phenomenon (Burke et al., 2006; Han & Williams, 2008). To elaborate:

- **Proactive and reactive components.** In describing whether an individual is more or less “adaptable,” the most comprehensive framework was developed by Pulakos and colleagues (2000; Dorsey et al., 2017), who identified eight dimensions of adaptive performance (p. 617):
  - Handling emergencies or crisis situations
  - Handling work stress
  - Solving problems creatively
  - Dealing with uncertain and unpredictable work situations
  - Learning work tasks, technologies, and procedures
  - Demonstrating interpersonal adaptability
  - Demonstrating cultural adaptability
  - Demonstrating physically oriented adaptability

- These eight dimensions can be described as more proactive or reactive in orientation, such that, for example, “handling emergencies or crisis situations” can be described as an adaptive reaction to the environment, while “learning work tasks, technologies, and procedures” can be described as a proactive method of adapting to future requirements (Huang et al., 2014).

- **Context dependence.** The specific nature of adaptation needed will depend on individual circumstances and the organizational context. For example, jobs with high physical requirements, such as with law enforcement or military personnel, are more likely to need physically oriented adaptability, while those working in international contexts are more likely to require cultural adaptability. Thus, while there are antecedents and processes (described below) that will increase adaptability in general, the most effective adaptations are likely to be context-specific.

- **Adaptability as multi-level.** Since early work by Pulakos and colleagues (2000), scholars have begun to apply the concept of adaptability at the team and organizational levels (see, for example, Burke et al., 2006; Hatwig et al., 2020; Hillmann & Guenther, 2021; Maynard et al.,

---

\(^{18}\)https://www.cisa.gov/sites/default/files/publications/HRs%20Role%20in%20Preventing%20Insider%20Threats%20Fact%20Sheet_508.pdf

\(^{19}\) When emphasizing different aspects of adaptability or particular domains, the terms “flexibility,” “resilience,” and “agility” are also used. For consistency, we use the term adaptability throughout this section.
2015; Raetze et al., 2021; Stoverink et al., 2020). Multi-level models are common in social science research (e.g., Dansereau & Yammarino, 2003; Mumford & Hunter, 2005), recognizing that unique antecedents and processes are needed to describe the effectiveness of the same concept at different levels. At these levels, adaptability is generally defined by measures of effectiveness instead of performance dimensions such as those described above. For example, team performance can be defined by a return to a baseline after an incident or change that impacts performance (cf. Burke et al., 2006; Hartwig et al., 2020). Team adaptation is also sometimes measured by member impressions of team adaptability, such as with a team adaptability scale developed by Marques-Qinteiro and colleagues (2015) that relies on the Pulakos et al. (2000) dimensions shown above. Similarly, organizational adaptability is frequently described by overall firm performance (e.g., Pulakos et al., 2019) or recovery from a disruptive event (Hillmann & Guenther, 2021).

We turn our attention now to factors that enhance adaptability at the individual and team levels. We focus on these two levels because they are most relevant to identifying potential positive deterrents to insider threat.

**Antecedents of Adaptability**

There is a substantial body of literature on antecedents of adaptability at all levels that can generally be classified in one of two ways. The first is distal antecedents indicative of adaptability that are stable/difficult to change without significant effort. The second is process-focused antecedents that are easier (relative to distal) to change and impact adaptability outcomes. These antecedents are not mutually exclusive—changes in processes can have a positive impact on distal antecedents for example. However, the distinction between distal and process-focused is useful for distinguishing variables to estimate baseline adaptability (distal) vs. driving new organizational policies to enhance adaptability (process-focused). As we examine the evidence for these antecedents at each level (individual, team), we find more empirical support for those identified at the individual than at the team level. We briefly summarize this research and its implications below.

**INDIVIDUAL-LEVEL FACTORS.**

The distal and process-focused individual-level factors most likely to predict individual adaptability depend on the proactive and reactive components needed for the target job. For example, general mental ability (Dorsey et al., 2017), having a learning/mastery orientation (Bell & Kozlowski, 2008), and achievement striving (Griffin & Hesketh, 2005; Huang et al., 2014; Pulakos et al., 2002) are all thought to be distal predictors of adaptability. The primary mechanism for this relationship is through (a) the proactive process of learning new work tasks, technologies, and procedures; and (b) the ability to handle uncertain situations through learning. Similarly, knowledge (domain knowledge, broad knowledge, situational knowledge; Schmitt & Chan, 2006; Hunter et al., 2012; Mumford & Hunter, 2005) and openness to experience (Griffin et al., 2007; LePine et al., 2000) are also thought to be related to adaptability through research demonstrating their connection with solving problems creatively. The key takeaway from this literature is organizations that understand the adaptability demand characteristics of the roles within their organization are more likely to be able to select employees who are most likely to thrive in those roles.

In addition to these distal factors, there are process-focused actions that can be undertaken by individuals to increase their adaptability. For example, employees well-trained on their technical tasks will have high (a) task knowledge and (b) self-efficacy (i.e., confidence in the ability to complete a task), both of which are related to adaptability in learning settings (e.g., Bell & Kozlowski, 2008). General positive attitudes and emotions are also predictive of adaptability (cf. Raetze et al., 2021), as are
specific stresscoping strategies, such as help-seeking behaviors (Britt et al., 2016). Organizational wellness programs, such as those that encourage healthy diet, sleep, exercise, and mindfulness habits are likely to have similar positive effects. These process-focused factors can be developed (e.g., through training) and encouraged (e.g., through policies and programs) by organizations to increase individual employee adaptability and, by extension, reduce the negative factors predictive of insider threats.

**TEAM-LEVEL FACTORS.**
Research into team-level adaptability tends to focus on reactive forms of adaptability rather than proactive, with the notable exception of the robust literature on team creativity (Anderson, Potočnik, & Zhou, 2014; Mumford & Hunter, 2005). In reviews of team adaptability, the first factor generally considered critical to building capacity is team climate and culture. A scholarship supports two interrelated concepts as being important distal antecedents of adaptability—(a) psychological safety, or the ability for team members to speak up without fear of reprisal (Ravishankar, 2022), and (b) continuous learning, or a culture that promotes reflection and development (Han & Williams, 2008). Similar to the role that learning/mastery orientation plays at the individual level, a continuous learning orientation at the team level is thought to improve team adaptability through knowledge acquisition by members, knowledge dissemination, and the ability to continuously update team mental models to solve problems (Han & Williams, 2008; Stoverink et al., 2020). Psychological safety is important during periods of uncertainty as open communication allows team members to make sense of the situation, plan, and take action (Burke et al., 2006; Stoverink et al., 2020).

This leads to another antecedent of team adaptability—team shared mental models, including the collective understanding of (a) tasks and resources needed to complete team objectives, (b) team member roles and responsibilities, and (c) team member knowledge, skills, strengths, and weaknesses (Mathieu et al., 2000). Shared mental models allow team members to quickly determine the next course of action in uncertain or unpredictable situations. Finally, team positivity and efficacy—the confidence that the team can address challenges—also help teams to better manage difficult or stressful situations (Raetze et al., 2021; Stoverink et al., 2020). In terms of processes, Burke and colleagues (2006) and Rosen and colleagues (2011) emphasize the criticality of planning behaviors in increasing team adaptability. This includes processes such as environmental scanning, developing effective plans, contingency/scenario planning, and taking deliberate steps to continuous improvement.

The underlying implication of the above section is, following propositions by Moore et al. (2022) and Dorsey et al. (2020), that adaptable individuals and teams are significantly less likely to generate an insider threat than less adaptable individuals and teams. The mechanism for this is positive deterrence—adaptable individuals and teams have positive outcomes (e.g., performance, commitment, wellness) even in adverse circumstances. If supported, this observation would have significant implications for addressing insider threats through policies that increase individual and team adaptability.

**Key Takeaways from Part 2**
From our review of the practitioner-oriented and social and behavioral science literature in Part 2, we can take away the following as it applies to insider threat:

**Takeaway 1: The practitioner-oriented literature, in conjunction with the literature reviewed in Part 1, can deepen our understanding of malicious insider threat risk.**
The practitioner-oriented resources suggest some overlap and some unique indicators of threat across types. For example, the resources related to espionage, sabotage, and workplace violence all suggest the importance of underlying grievance or disgruntlement and the presence of triggering events. However, as an example of a unique motivation, perpetrators of espionage (particularly leakers) are
more likely, according to this literature, to be driven by narcissistic tendencies, such as playing the role of an expert (Thompson, 2018), while perpetrators of workplace violence are more likely to be motivated by narcissistic injury, and turn to violence as a way to restore personal honor (White, 2021). This supports the “pathways” idea described in Part 1 (Lenzenweger & Shaw, 2022). An important implication of this observation is the potential that different counter-insider threat organizational policies or interventions could potentially be oriented towards different types of malicious insider threat.

Implication of takeaway 1: Models of insider threat should explicitly account for probability differences in risk indicators by types of malicious threat events.

Takeaway 2: The social and behavioral science literature points to new potential methods for mitigating insider threat risk.
Specifically, the political violence and terrorism/targeted violence literature deepens our understanding of the role ideology and group membership can play in insider threat risk. This is critical as the role of these factors is under-represented in models of insider threat discussed in Part 1, and suggests new potential interventions, such as attention to engagements with AGAAVE and REMOVE ideologies. The CWB and adaptability literature both suggest organizational interventions that could be used to expand on the models presented in Part 1 and also suggest new interventions. For example, the adaptability literature suggests several potential avenues for increasing resilience at all organizational levels, providing potential positive deterrence factors against threat events. As a second example, both literature point to the potentially crucial role of leadership in insider threat mitigation. Effective leadership at all levels improves a wide range of relevant outcomes, including lowering instances of CWBs, improving ethical behaviors, improving organizational climate and culture, and many others.

Implication of Takeaway 2:
Models of insider threat, and particularly positive deterrence counter-insider threat approaches, can be further informed by additional literature in the social and behavioral sciences.

Conclusions and Next Steps
The purpose of this report was to review extant literature related to insider threat to inform the larger threat assessment practice. In Part 1, we reviewed literature specifically related to insider threat, with a particular emphasis on the information systems and technologies (IS&T) field. We found that IS&T models of insider threat could be used to inform threat assessment research and practice. However, there were limitations to these models as they relate to threat assessment, such as less consideration of multi-factor threats, over-reliance on network-based indicators, and a lack of specificity in prevention-focused solutions. To address some of these limitations, we examined practitioner-oriented and behavioral and social science literature related to insider threat. From the practitioner perspective, we learned that there are both overlapping and unique factors in the antecedents and situational factors predicting acts of espionage, sabotage, and workplace violence. From the social and behavioral science literature, we learned that there are a variety of steps organizations can take to prevent threat events that are not currently well-specified in the literature.

The first two parts of this report are part of a larger effort to better understand insider threat and information threat assessment practice. Future work will add two more parts described below:

In this effort, we will systematically analyze the above literature to better inform our understanding of workplace violence, espionage, and sabotage. We plan to accomplish this by leveraging systematic
reviews (e.g., narrative reviews, meta-analyses, technical summaries) in each literature area from Parts 1 and 2 to build specified models, including proximal and distal antecedents and associated mediating and moderating relationships, of each threat type.

**Future Part 4: Prevention-Focused Solutions.**

From the literature reviews and models from Future Part 3, we will offer a set of recommendations for potential solutions. Our recommendations will focus on early prevention interventions, as most of the extant literature in both counter-insider threat and threat assessment either (a) catch malicious behavior in the act (e.g., someone installing a backdoor for off-network access) or (b) involve late-stage preventions, such as intervening when someone exhibits behaviors of concern. Our goal is to develop solutions that inform policymakers and researchers in this space.
Blind Spot D: Mitigating Threat Fixation – The Unique and Harmful Impact of Novelty on Threat Assessment

The last blind spot explores the potential for removing a fixation with common threats that individuals conducting threat assessment tend to have. To do this, the organizational sciences were utilized to explore the bias against originality phenomenon people may exhibit when evaluating the likelihood and/or severity of novel threats.
Overcoming a Bias Against Novelty in the Evaluation of Threats

NCITE Center Research Team

Sydney Reichin – University of Nebraska at Omaha
Kelsey Ciagala – University of Nebraska at Omaha
Kat Parsons – University of Nebraska at Omaha
Alexis d’Amato – University of Nebraska at Omaha
Sam Hunter – University of Nebraska at Omaha
Introduction

“It comes back to the fact that the policies and procedures of the Secret Service are born out of blood,” he said. ‘The Service will get better once it’s tested. Every time it is tested, it gets better. As the global threat environment constantly changes, the Service has to change in response.’”

-Carol Leonnig, Zero Fail: The RiseAnd Fall of the Secret Service, p. 242

Effective threat assessment and threat management (TATM) is key to preventing targeted violence and terrorism. The first step in TATM is the evaluation of potential threats utilizing behavioral threat assessment and management (BTAM). Promising practices indicate that an interdisciplinary team of psychologists, law enforcement, managers, and other potential stakeholders, utilize Structured Professional Judgment’s (SPJs), assessment tools designed to guide threat assessors in their evaluation. This often involves an assessment of the individual posing a threat including patterns of behavior and behavioral warning signs, risk factors, protective factors, and precipitating events (JCAT, 2023; NCTC, 2023). Once the threat has been evaluated, a mitigation plan is developed to reduce the risk of violence, both in the short and long-term. As such, this also includes “relentless follow-up” (NCTC, 2023). Many risk assessments have been created that are tailored to different potential threats to help with this mitigation process (NCTC, 2023). While the entire TATM process is crucial, the focus of this paper is the evaluation piece of threat assessment.

We posit that barriers exist due to a bias against originality that stifles the security workforce’s ability to evaluate potential threats, especially threats that are novel. We see these barriers not only across the Homeland Security Enterprise (HSE) but society and organizations in general. Unfortunately, despite identifying an increasing need for creativity in modern society, studies find that many individuals and organizations are resistant to novelty and novel thinking in varying ways. Scholars have termed this phenomenon the originality bias – where individuals tend to favor what is familiar and prototypical, often rejecting the most unique ideas presented (Hunter et al., 2022; Licuanan et al., 2007; Mueller et al., 2012; 2014). In society and organizations, this resistance to new ideas is unfortunate given the many benefits stemming from innovation and creativity. Consider companies like Tesla, Toyota, and BYD who have emerged as innovation leaders in the electric vehicle market. The innovations of these companies have made cars available that improve fuel economy, lower fuel costs, and reduce harmful emissions, yet all have faced resistance when novel approaches have been presented. Central to the discussion here is the realization that such innovations would not be possible if organizations were not able to address and ultimately overcome originality bias. The resistance to new ideas could prove even more important to address in the security workforce given the high-stakes ramifications of TATM. As such, the current paper will outline how we can apply decades of research in the creativity literature on idea evaluation, in concert with research in the organizational sciences, to address these barriers to evaluating novel threats.

Introduced in the 1990s, the 8-stage model of creative problem-solving describes the processes contributing to the generation of innovative problem solutions (Mumford et al., 1991). This process begins with problem construction and “ends” with implementation and monitoring of some solution, encouraging individuals, groups, or organizations to cycle through previous stages of the process when needed. The intermediate process of most relevance to the evaluation of potential threats is, of course, idea evaluation, which plays an important role in creative thought and achievement (Dailey & Mumford, 2006). Idea evaluation contributes to the creative process in several ways. First, evaluating ideas allows employees to identify viable ideas that are worth pursuing, thus resources can be dedicated appropriately (Simonton, 2003). Second, ideas can be reshaped into viable options, as teams improve...
their potential and enhance their workability (Csikszentmihalyi, 1999). Finally, appraisal and revision of ideas may act as a catalyst for continued creative thought (Lonergan et al., 2004). As alluded to earlier, however, there is the risk of originality bias emerging when evaluating ideas.

Specifically, we posit that a bias against originality can make it difficult for individuals to evaluate ideas effectively. Consider when Steve Jobs announced the first iPhone at Macworld in 2007. What if the employees of (then) Apple Computer Inc. heard the idea to create a touch-screen phone with no keyboard and decided it was a bad idea? We still might be walking around with a BlackBerry with a physical QWERTY keyboard. Although Apple and Jobs were able to readily address and overcome the originality bias, other organizations and industries have faced significant challenges and biases. When Alexander Graham Bell first introduced the telephone, for example, there was little interest in the technology – most notably Western Union who turned down an offer to buy the patent of the nascent product. The Beatles, known for their groundbreaking sound and record-setting rise, were initially rejected by several record labels. Funders were not interested in giving the young director, George Lucas, money to support his genre-creating film, Star Wars. Even the seemingly sacred destination of Disneyland faced early and significant skepticism with investors shying away from funding the project. The point is this: Even the best and most benevolently intended novel ideas have avoided significant skepticism if not outright rejection.

The examples touched on above showcase how innovation can serve as a catalyst to improve or at least entertain society, but novel ideas can have a darker side. Consider those individuals or groups that seek to cause harm and disrupt societal ways of life. Creativity is valued even in malign contexts that include terrorism and targeted violence (Gill et al., 2013). Creativity to intentionally harm others is defined as malevolent creativity (Crapley et al., 2008; Hunter et al., 2022) with malevolent innovation representing the implementation of malevolently creative ideas. Crenshaw (2010) describes a similar concept, the tactical innovation of terrorists, where the technologies used to carry out an attack are innovative. Logan et al. (2019) expand our understanding of tactical innovation by examining dimensions of innovation in a sample of attacks. They find that there are three dimensions of innovation: novelty, relevance, and elegance. Much like traditional organizations, creativity, and innovation are also critical for the success of terrorist organizations. Like traditional organizations, terrorist organizations also feel the pressures of market demands and are housed in turbulent environments. Effective counterterrorism policies put in place by counterterrorism agencies, as well as competition from other groups with similar goals, add pressure to ideate creative solutions to further their goals (e.g., causing harm). Additionally, characteristics of organizational leadership (e.g., expertise, participatory decision-making) and characteristics of the organizations themselves (e.g., decentralized structure, rewards, collaboration; Gill et al., 2013) encourage creativity and innovation.

As terrorists become more innovative and creative, however, so too should the security workforce (d’Amato & Hunter, 2023). Innovative terrorists ideate and execute creative and innovative attacks. The collection of such intentionally violent activities and the preparation for them constitute the notion of novel threats. The novelty of these threats leaves counterterrorism approaches potentially deficient in their ability to thwart attacks, leaving many inadequately prepared and vulnerable. Counterterrorism efforts are often successful because the security workforce in the United States is aware of many common types of attacks. As such, members of the HSE have learned how to successfully predict and guard against these attacks. Perhaps, to a fault.

“The Secret Service’s best methods, agents often say, are developed in the wake of a crisis, a teachable moment that exposes a weakness. Every assassination attempt or attack reshaped the agency’s tactics and shored up its defenses against a threat the Service has previously failed to foresee or address.”
As illustrated in the quote above, those working in the security community innovate and adapt in the wake of significant harm. Although this innovation and adaptation in response to tragedy is commendable, it is also unfortunate that creative thinking and action are in response to catastrophe striking, rather than successfully thwarting certain attacks before they occur. Often, members of the HSE are engaging in good faith and expertly guided efforts to guard against emerging threats. Rather, the central novelty of such attacks highlights deficits in their standard preparation. We offer that an originality bias can lead to the ineffective evaluation of novel ideas in a threat-based environment. In other words, if the security workforce does not recognize threats that are novel, we may be under-protected. Consider the following historical example:

A stolen propeller plane crashed on the White House lawn in the fall of 1994 resulting in a sizable shift in how aircraft threats were perceived. Specifically, as a result of the investigation following the crash, Tigerwall, a new classified program, was adopted. This program allowed the Secret Service to monitor FAA’s real-time radar when planes were suspiciously close to downtown Washington’s restricted airspace, providing the Secret Service with access to early warnings if a stolen plane ever headed toward the White House again.

Yet on 9/11, the early warning of two planes suspected of being hijacked was headed in the direction of Washington and as little as 30 minutes out. This warning did not make it to Secret Service leadership until 20 to 30 minutes after the initial warning from the FAA. At that point, the Service was sorely underprepared to do anything other than try to evacuate the White House. Indeed, if United Airlines Flight 93 – the fourth hijacked plane on 9/11 – made it to its intended target of the White House or the Capitol, Program Tigerwall would have done little to help. Additionally, because of the damage that would result from bringing down a plane in downtown Washington, there was little that could be done in terms of antiaircraft weaponry. Although more prepared against the hijacking of a small propeller plane, the novelty of hijacking a large passenger airline was outside the scope of what the USSS had prepared for. The originality of the attack was a key factor in the failure to appropriately circumvent the threat.

Today, commercial plane hijacking is relatively rare, thanks to tighter airport security precautions based on lessons learned from 9/11. Indeed, as novelty decreases, preparedness increases (Cropley et al., 2008). However, the goal of this effort is to provide promising practices and guidelines to the security workforce to overcome a bias against originality, so they are better able to predict and make appropriate decisions about novel threats, rather than just learn from the disastrous aftermaths. We offer that rather than being born out of tragedy, successfully defending against violence can be born out of innovation.

To make this goal a reality, we need to understand how those working in the Homeland Security Enterprise (HSE) can better identify, and make decisions about, novel threats. As alluded to above, we postulate that originality bias is a key barrier to detecting novel threats. This paper will outline how work in organizational psychology and management can offer some potential avenues to overcome an originality bias. Specifically, we will first discuss reasons for resistance to new ideas and then how lessons learned from organizational psychology and management can inform how to overcome that resistance. These lessons can be applied to the broader security workforce to mitigate this resistance to novelty and originality. In turn, these individuals will be better positioned to predict and protect against novel threats.
Resistance to Novelty: Unpacking the Originality Bias

There is empirical support for the notion that many are resistant to novelty, in that many individuals support ideas that are in line with social norms and thus reject highly original ideas (Blair & Mumford, 2007; Mueller et al., 2012; Mueller et al., 2014; Mueller & Yin, 2021). Despite these established linkages, there remains a lack of clarity around precisely why this is the case. As such, we outline different explanations for this bias against originality and specifically outline how these explanations may affect the evaluation of novel threats.

The social information-processing model of creative idea evaluation will act as our organizing framework (Watts, 2023). This model of creative idea evaluation posits that three social context factors may influence how an idea is evaluated. These factors include characteristics of the idea (e.g., risk, usefulness), characteristics of the evaluator (e.g., expertise, traits), and characteristics of the context (e.g., evaluative standards, environmental constraints). We organize our thoughts on barriers to evaluating novel threats into a similar framework, where characteristics of the novel threat, characteristics of the evaluator, and characteristics of the context all impact how a novel threat is evaluated (See Figure 1).

![Figure 1. Social-information-processing model of novel threat evaluation (adapted from Watts, 2023).](image)

**Novel Threat Characteristics**

The first social context factor that may impact the evaluation of the novel threat includes characteristics of the novel threat itself. Watts (2023) posits that characteristics of the idea, including perceptions of the idea source, can impact the evaluation of it. As an extension, the perception of the novel threat source can impact the evaluation of the novel threat. Consider the following examples:

**Perceptions**

After eight months on the job, Secret Service officer Charles J. Baserap made several observations about the state of security at the White House. He had many ideas about improving security including, but not limited to, replacing the use of handguns, improving the communication from post to post at different parts of the complex, and restructuring where inexperienced and experienced officers were assigned. Joseph Clancy, the number two in charge of President George W. Bush’s detail, said to Baserap, “You think you have these great ideas. But you haven’t been here long enough to know what you don’t know. You don’t have the big picture” (Leonig, 2021, p. 292). After presenting these ideas about potential security threats, the USSS decided not to renew Baserap’s contract right before he reached career status. From such interactions, it seems reasonable to assume that during this era, the culture of the USSS was one unsettled by officers or agents questioning the way things were done. For Baserap, the
perception that he was too much of a novice to understand security gaps, or perhaps too novice to be perceived credibly, made it so the threats he proposed were not seen as credible. In another example that ultimately led to the protective mission set of the USSS, Lincoln was warned by Charles Colchester about Booth’s plan to assassinate him. Turns out, Lincoln and Booth shared this acquaintance. Colchester happened to work as a clairvoyant, and this, on top of his odd personality, likely impacted Lincoln’s perceptions of Colchester as a credible source. However, Colchester’s intel was not spiritual, instead, it came directly from Booth on a night out drinking (Alford, 2015; Ali, 2023). Although other examples exist, the takeaway is that perceptions of the threat play a significant role in our dismissal, or acceptance, of them.

Fear
Another characteristic of a novel threat that may impact its evaluation is how fear-inducing it is. In other words, the ambiguity and uncertainty around novel threats can often result in anxiety and fear or other aversive emotional states. As a result, when presented with a novel threat, we may seek decisions that provide us with quick comfort. In this case, the decision may be that the threat proposed is not credible, because if it is not credible, it cannot induce fear. For example, some purport that the discovery of extraterrestrial life is growing increasingly plausible (e.g., Kaufman, 2022), and while the majority of U.S. adults say their best guess is that intelligent life does exist on other planets, over a third of U.S. adults do not believe this to be the case (Pew Research Center, 2021). Why do so many discount the possibility? It could be that for some, acknowledging that extraterrestrial life could exist is just too frightening. Instead, these individuals likely search for evidence for the contrary, or use ill-fitting criteria to evaluate the claim. The same is true for proposed novel threats.

Heuristic access and interpretability
Finally, the ease at which one can discuss a novel threat may be another characteristic of a novel threat that may impact its evaluation. In other words, there is a lack of language with which to discuss novel threats. Because these threats are new, it may be difficult to articulate how such a threat could exist and difficult to understand the potential consequences. Indeed, how an idea is pitched affects the perception of the idea. Research shows that high-quality pitches can improve enthusiasm for an idea, and this is especially true for highly original ideas (Hunter et al., 2022). As such, the ease at which the threat can be discussed will have a clear impact on its evaluation.

Consider the discussion of cyber-attacks by terrorists in the early 2000s. Cyber-attacks against critical infrastructure were certainly acknowledged as a possibility, but the threat was often dismissed, considered “far-fetched” (Wallace, 2002), or a “myth” (Green, 2001). Because we had yet to experience such an attack, those who did take the threat of cyber-attack seriously had to look to imperfect heuristics to assess the immediacy of the threat and the potential consequences of such a threat. As such, to gauge the effect of cyber-warfare, experts needed to look to other sources such as non-terrorist cyber-attacks against infrastructure and the effect of routine infrastructure failures. For example, the Center for Strategic and International Studies referenced the economic cost of months of blackouts and rolling brownouts in California in 2001 (Lewis, 2002). However, they note that these blackouts were not crippling and did not strike terror into the hearts of Americans, implying that a terror attack causing a blackout would not lead to serious consequences. It was only the next year that the Northeast saw the devastating consequences of the Blackout of 2003, killing electricity to more than 50 million people in the US and Canada. This blackout directly or indirectly contributed to the death of many due to carbon monoxide poisoning, triggering heart attacks, and aggravating respiratory conditions. While most believe the blackout was not a terror attack, the consequences of a terrorist cyberattack were now thought of as more dire than previously thought.
Evaluator Characteristics

Diversity of expertise

Along with the characteristics of the threat itself, the characteristics of the evaluator may also play an important role in how a novel threat is evaluated. Specifically, the expertise of the evaluator, or expertise that the evaluator seeks out, will impact how a threat or idea is evaluated. Given the unique nature of novel threats, however, there are typically few experts available to provide insight into such threats. That is, because we cannot have expertise in what does not yet exist, it is difficult for evaluators to use their own expertise or look to others’ expertise when evaluating a novel threat. There are no experts in alien weapons technology because we don’t know what an alien might use. If extraterrestrial beings landed on the front lawn of the White House, there is no established expert to call for input and guidance and those who would purport to know would be guessing along with the rest of us.

Because there are no single experts available to assess genuinely novel threats, one solution may be to pull a group of individuals together with diverse expertise. Indeed, the best practice in TATM is to establish a multidisciplinary threat assessment team (NTAC, 2018). The composition of these evaluation groups can have a direct impact on the evaluation of a threat. For example, a combination of individuals with different backgrounds evaluating a threat may find it difficult to discuss, especially since novel threats already lack available language (one of the novel threat characteristics discussed previously) as well as lacking in the core expertise needed to evaluate the threat. As such, although a step in the right direction, the use of teams may not be efficient or wholly effective in overcoming biases when evaluating a novel threat.

Emotions

As discussed earlier, novel threats may evoke fear or other aversive emotional states thereby negatively impacting the evaluation of novel threats. It is useful, however, to more fully unpack the role each evaluator and their unique emotions play in understanding threat evaluation and response. For some evaluators, the discovery of a novel threat may evoke energizing emotions such as anger (that an attack like that could happen) or variations on elation (that steps can now be taken to prevent such an attack). Mueller et al. (2012) note that those who experience anger and happiness are often more tolerant of uncertainty and, as a result, are less susceptible to originality bias. However, although energizing emotions like anger and elation can drive engagement in thinking through an idea fully, some evaluators may be fearful of the thought of such a threat. Fear, in contrast to emotions like anger, can be aversive and drive evaluators to avoid the emotion. Indeed, Lee et al. (2017) found that individuals who have fearful responses to an idea have an increased bias against creativity, leading to decreased creativity ratings of the idea. So, it seems that fearful individuals perceive more uncertainty and are less tolerant of uncertainty than those who react to novel ideas with emotions like anger or happiness.

Accountability pressures

Another characteristic of the evaluator that we propose will affect novel threat evaluation is evaluator pressures related to being held accountable. Indeed, Mueller et al. (2018) found that decision-makers in charge of assessing creativity have an economic mindset evoked because they are responsible for allocating or withholding resources for creativity. Because of this mindset, evaluators are focused on concerns at the heart of economics, such as how acceptable an idea is. Given we are talking about novelty, it seems to reason that this responsibility becomes challenging because of how uncertain novel ideas are. Indeed, Mueller et al. (2018) found that because of this economic mindset, decision-makers look for cues that signal the acceptability of an idea, specifically, social approval for an idea. When social approval is low, because of this economic mindset, these decision-makers may rate ideas incorrectly. In a similar vein, Harvey and Mueller (2021) discuss how often it is consensus-based
problem-solving groups that make decisions about novelty. These groups are accountable to others in the organization if their recommendations fail. As such, these groups may prioritize predictability and correctness over potential novelty. In the case of novel threats, pressures of the evaluator to be held accountable for which novel threats are taken seriously may impact how they evaluate the threats proposed.

Indeed, we have seen historical examples where the mindset of the evaluator impacts how a threat is perceived. Abraham Lincoln and John F. Kennedy were similar in that they prioritized “being amongst the people” over their own security. Many of Lincoln’s friends had been concerned about the adequacy of his security, but due to Lincoln’s insistence on being amongst the people, Lincoln disregarded his friend’s worries (Alford, 2015). Similarly, Kennedy had a reputation in the U.S.S.S for having a blatant disregard for following the rules and being stubborn. Unfortunately, this would be his downfall. Agent Jerry Blaine, an agent in charge of preparing for a string of appearances in Florida (directly before Kennedy’s trip to Dallas) recommended that two agents ride on the rear steps attached to the back of Kennedy’s open-air Lincoln Continental for the entire ride through various cities. Kennedy did not like this, he believed it to be excessive. He says to his agent, “It’s giving the wrong impression to the people. Tell them to stay on the follow-up car. We’ve got an election coming up. The whole point is for me to be accessible to the people.” (Leonig, 2021, p. 51-52). By having this mindset, Kennedy disregarded recommendations from his staff. At Kennedy’s request, no agents were riding on the rear steps attached to the back of Kennedy’s car while driving through Dallas. Instead, Agent Hill was stationed at the front of the follow-up car:

“With the first shot, he had jumped off the follow-up car and was now running for the back of the limo. He stumbled, then grabbed hold of the trunk handle. A third shot rang out, which Hill not only heard but felt. The right side of the president’s head exploded, a pinkish spray rising up near his ear, and he slumped over on his left side onto his wife.”

– Carol Leonig, Zero Fail: The Rise and Fall of the Secret Service, p. 59

If Hill had been in the back of the car as recommended, he may have been able to shield Kennedy. In each of these examples, the presidents refused to evaluate the novel threats shared by their security seriously.

Context Characteristics

Evaluative goals and standards

Finally, characteristics of the context will also impact the evaluation of novel threats. One context characteristic that Watts (2023) includes in the early model is evaluative goals and standards. We consider this to be the biggest barrier facing the evaluation of novel threats. Specifically, evaluative goals and standards for novel ideas do not exist in the same way that evaluative goals and standards exist for less original ideas (Licuanan et al., 2007). For example, in the evaluation of ideas, decision-makers often rely on a frame of reference or past experiences. Reiter-Palmon and Illies (2004) refer to this as the “yardstick against which the solution is being evaluated” (p. 71). Not surprisingly, this is more cognitively demanding when evaluating novel ideas where no such frame of reference exists (Hunter & Ligon, 2022). Imagine that someone hands you a tablet – you can easily compare the tablet you are holding to other tablets you have held. Maybe the resolution is better, or the screen is bigger, or it is lighter than another tablet. Now consider the first iPad, what most consider to be the first widely used tablet, that Apple launched in 2010. When the iPad was launched, you could compare it to a phone or a laptop, and in doing so, evaluations would be poor. The first iPad would be viewed as a phone that doesn’t fit in your pocket or as a weaker laptop. Because there were no tablets to make the comparison
against (e.g., is this the highest resolution or cheapest tablet) it was difficult to conclude the viability of the product. Even purported experts claimed that Apple’s tablet would fail. Some claimed that it would fail because the lab is a bad desk, people would miss keyboards, and it would not be able to compete with new, lightweight, sleek laptops (Kennedy, 2009). Contrary to predictions, Steve Jobs ensured that the device would be better at certain tasks than a laptop or a smartphone, such as better web browsing, email, photos, video, music, games, and ebooks (Warren, 2020). This added cognitive complexity, making it much harder to evaluate the product. Just as the first iPad was likely difficult to evaluate, so too are novel threats. Consider another example:

The Secret Service has long been protecting Presidents against assassination. Assassins most often held grievances against a President and used that grievance as their reasoning for assassinating, or attempting to assassinate, a President. Because of this, the Secret Service disregarded threats from mentally unstable individuals without grievances, who wanted to kill for fame. John Spencer Daughetee slid under the Service’s radar because they decided he was “confused” and didn’t add him to the database of dangerous people to check in on periodically. Daughetee tried, on three different occasions, to assassinate Vice President Bush. He honed plans for four years before he was eventually caught (L.A. Times Archives, 1989). Because of the heuristic available to the Service, Daughetee was not considered a threat.

Consider a consensus-based group evaluating novel threats. These groups rely on known criteria that are easily accessible and defendable to the group. Harvey and Mueller (2021) use the example of the first digital camera. Experts in film decided the digital camera would not be useful because the picture quality was poor. These experts did not anticipate that consumers would find the cheaper price and immediate gratification to be more useful than the quality of the picture. Because these experts only had film as the evaluative standard ready to compare the digital camera to, they evaluated the idea as low in usefulness.

**Environmental constraints**

Environmental constraints are another important consideration. These are external constraints that originate from factors outside an individual’s control. The first of these constraints is access to resources. Consider the example above – not only do these experts not have easily accessible criteria, but also lack the time, effort, and resources to ideate better criteria or evaluation standards with which to judge novelty. Thus, taking these shortcuts and evaluating new things against previous models makes sense because they simply do not have the resources to become experts in something new.

In addition to resources, other environmental constraints make the whole process of predicting the credibility of a novel threat more challenging. This is because of the tension between novelty and predictability of how useful something will be (Harvey & Mueller, 2021). To reduce this tension, many evaluation groups will use prototyping or experimentation to gather information about how useful an idea is. This is simply not helpful in the context of evaluating novel threats, whereas it may be useful when evaluating a novel product.

**Organizational climate**

Another contextual characteristic includes the climate of the organization. Hunter and Ligon (2022) acknowledge that it can be uncomfortable or embarrassing to discuss novel ideas (see also Hunter & Cushenberry, 2015). Because we generally care about how others perceive us, individuals might feel uncomfortable or embarrassed when sharing an opinion on a novel idea. Thus, the climate of the organization, and how psychologically safe employees feel to share new things, will absolutely impact how a novel threat is evaluated – in part because it will impact if a novel threat is even proposed.
Discussing a novel threat without the ability to make the case using established criteria puts us at risk of ridicule from their team or seeming unintelligent. Thus, individuals fail to discuss their hunches or wildest theories when that is necessary to identify genuinely novel threats.

Competing ideas
Finally, competing ideas will impede the evaluation of novel threats. For example, a bulletproof glass manufacturer who is put out of business by a new weapon that can circumvent that protection will not be motivated to recognize a threat that makes them obsolete. Multiply that small instance by a factor of 100 and you can see incentive structures in place to retain the status quo and will impede the evaluation of novel threats. Consider how tobacco companies were motivated to hide the finding that smoking causes lung cancer. The same may be true for novel threats.

We are naturally inclined to dismiss or avoid novel ideas, and the same may also be true for novel threats. However, not all is lost. We posit that there are ways to combat this bias against originality, and we will draw on the organizational psychology and organizational creativity literature to support this notion.

Lessons from Organizational Psychology and Management
In the following section, we will discuss how lessons learned from the organizational sciences can be applied to overcome the proposed explanations for a bias against originality. Specifically, we discuss how the security workforce can apply lessons from leadership, teamwork, organizational climate, and human resources research. Specifically, we will refer back to the social-information-processing model of novel threat evaluation to discuss how lessons can address evaluator characteristics, novel threat characteristics, and context characteristics that impact novel threat evaluation.

Leadership
Lessons from the organizational sciences related to leadership can address evaluator characteristics and context characteristics that contribute to a bias against originality. Specifically, leadership research can impact evaluator accountability pressures, available evaluative goals and standards, and organizational climate.

First, leaders may be able to alleviate some accountability pressures that employees feel when evaluating novel threats. As discussed previously, decision-makers look for cues that signal the acceptability of an idea (Mueller et al., 2018). As such, leaders can signal that it is acceptable to evaluate threats as novel and credible. For example, one way that leaders can enable and support the evaluation of novel threats, and therefore reduce accountability pressures, is through emotional intelligence. Specifically, Zhou and George (2003) propose that when leaders properly understand and then manage their emotions, they are less likely to dismiss ideas prematurely and more likely to evaluate an idea in an unbiased manner. Thus, if a leader in the security workforce can properly manage their emotions surrounding the evaluation of a novel threat, they may be able to react in ways that signal acceptance. In a similar vein, Liu et al. (2015) found that leader positive affect can lead to upward employee voice behaviors, such as expressing opinions that are different and pointing out problems in the organization (via employee positive affect and psychological safety). Advocating for the seriousness of a novel threat is not dissimilar from upward employee voice behaviors – these behaviors challenge the status quo, are risky, and might be seen as unpopular. As such, one way that leaders in the security workforce might alleviate accountability pressures is by displaying positive affect.

In addition to alleviating accountability pressures, leadership can help employees evaluate novel threats effectively even when goals and standards with which to evaluate novel threats do not exist. It is hard to
evaluate something where no “yardstick” or frame of reference is available. Reiter-Palmon and Illies (2004) concluded a review of the idea evaluation literature that the goals generated by a leader will serve as that so-called “yardstick” in the evaluation of ideas. Thus, leaders need to stress the importance of identifying novel threats so that evaluators use that as their frame of reference. In addition, because evaluating a novel idea is a cognitively demanding task, leaders need to provide intellectual stimulation to encourage innovative thinking (Hughes et al., 2018). Bass (1985) highlights that some ways that leaders can provide intellectual stimulation include challenging assumptions, taking risks, and soliciting ideas from followers. As such, leaders in the security workforce should start modeling these behaviors—challenging assumptions about what constitutes a credible threat, for example.

It is hard to evaluate novel ideas effectively if individuals are uncomfortable or embarrassed. Having a positive organizational climate may make employees feel safer in sharing these evaluations. Importantly, leaders play a pivotal role in cultivating a climate where employees are comfortable sharing risky and unpopular ideas. George and Zhou (2007) suggest that supervisors can provide a supportive environment for creativity by providing developmental feedback, displaying interactional justice, and being trustworthy. Even more, researchers find that creativity can be stimulated when leaders are supportive (Kim et al., 2010). So, not only may employees feel safer in discussing risky ideas, but they may also be better able to evaluate the novelty of the threat. As such, leaders in the security workforce have a responsibility to be supportive and make employees feel empowered to discuss novel threats without fear of being judged or ridiculed.

**Teamwork**

Given organizational psychology and management scholars have unique expertise in areas like teamwork, there are also important lessons we can apply to threat assessment teams that may help to overcome barriers in the evaluation of novel threats. Specifically, research on teamwork can address evaluator characteristics and context characteristics.

First, we can apply research on teamwork to help understand how to build a diversity of expertise in the evaluation of novel threats. Reiter-Palmon et al. (2012) highlight the importance of a team’s ability to effectively execute cognitive processes as a way to stimulate creativity. For example, one important cognitive process that teams need to execute is the exchange and elaboration of information—sharing ideas and knowledge among team members (Johnson et al., 2006). Interestingly, scholars have suggested that team composition factors can impact knowledge sharing and information elaboration in teams (Hu et al., 2017; Reiter-Palmon et al., 2012). A review of the team composition literature found that these include background diversity factors such as functional, educational, and occupational diversity (Hundscheidt et al., 2020). However, an important caveat is that these background diversity factors only stimulate creativity in teams where integration capability, open-mindedness, and prosocial motivation are also high. Given these findings, the composition of threat assessment teams should be carefully considered so that cognitive processes can function effectively. Especially given that the evaluation of novel ideas is already cognitively demanding, the security workforce should ensure that the composition of threat assessment teams is purposeful and thoughtful.

In addition to diversity of expertise, team research can contribute to our understanding of cultivating a team climate conducive to creativity. One of the contextual characteristics that we discussed that contributes to a bias against originality is organizational climate. Importantly, climates within teams (within organizations) will be equally as important for overcoming this bias. For example, a review of the team literature found that factors like participative safety and trust, support for innovation, and managing conflict and minority influence constructively have been shown to increase creative behavior in teams (West & Sacramento, 2012). These factors are all related to the idea of a supportive team.
Much like having supportive co-workers, supportive teammates will help team members feel safe to express ideas about novelty. Relatively, Byron et al. (2022) found that team collaboration is a key mechanism by which team creativity and innovation are possible. Specifically, Byron et al. (2022) found that team autonomy-supportive leadership (i.e., leaders providing structure to teams without inhibiting autonomy) and team task interdependence (i.e., tasks requiring coordination among team members) help teams become more collaborative.

It is important to note that just putting individuals together from different backgrounds and expecting creative thinking and innovative behavior can backfire without the proper team environment. First, information exchange and information elaboration are less likely to occur, especially in functionally diverse teams, when teammates experience low levels of psychological safety and trust (Gong et al., 2012; Newman et al., 2017). Team psychological safety can be understood as a shared belief in a team that interpersonal risk-taking in the workplace is safe to engage in (Edmondson 1999; Edmondson & Lei, 2014). As stated earlier, a major barrier to creative ideas and bringing those creative ideas to light is the inherent social risk (i.e., uncomfortable or embarrassing) involved (Hunter & Ligon, 2022). That is, psychologically unsafe teams will not remove any barriers in identifying novel threats and thus not reap the benefits teams have to offer.

**Organizational Climate**

The organizational sciences have long been interested in studying the climate of organizations. The extensive research on organizational climate will clarify how to overcome some of the context characteristics discussed that contribute to a bias against originality, including (of course) organizational climate as well as heuristic access and interpretability.

An organization’s climate encompasses employee perceptions of their work environment that shape their expectations, requirements, and interactions at work (Hunter et al., 2007). Importantly, much of this section echoes what we discussed previously – how supportive leaders can empower employees to voice their opinions about novelty. Importantly, however, climate is not only influenced by leadership. For example, positive interactions with co-workers are extremely important to building a climate where creativity is possible. In a meta-analysis of the relationship between climate dimensions and creativity and innovation, Hunter et al. (2007) found that positive collegial exchange was one of the strongest predictors of creative performance. Reiter-Palmon and Illies (2004) note that this positive collegial exchange is important for creativity because it allows for an open climate, where ideas are safe to be debated and discussed. This is further evidenced by Zhou & George (2001) who found that useful feedback from coworkers along with coworker help and support leads to more creative employees. The security workforce should focus on cultivating a climate where employees are supportive of one another, and where employees feel safe to express ideas about novelty without fear of embarrassment. In addition to a positive organizational climate contributing to a bias against originality, we also discussed how limited heuristic access and interpretability make it difficult to discuss novel threats. If an organization strives to foster psychological safety and a climate where employees feel safe taking risks, employees may be less concerned about making mistakes in the discussion of novel threats. This may make them more likely to discuss novel threats even if they do not necessarily know the best way to articulate their thoughts.

In addition to a supportive climate, it will also be necessary to cultivate a creative climate. A creative climate involves individuals and groups who perceive challenge and meaning in their work, share a sense of teamwork and commitment, and are defined by leadership, who encourage risk-taking via role modeling behaviors (Ekvall et al., 1983; Hunter et al., 2019). Because of this, a creative climate provides employees and teams with the necessary tactile and cognitive resources to explore the creative process.
(e.g., Hunter et al., 2019; Mumford et al., 2012), potentially making novel idea evaluation more effective. Researchers have found that several dimensions contribute to a creative climate (Amabile et al., 1996). First, both organizations and supervisors need to show encouragement. At the organizational level, this might include fair and constructive judgment of ideas, rewarding creativity, and mechanisms in place to support the development of new ideas. At the supervisor level, supervisors should serve as a good work model by setting goals appropriately, valuing individual contributions, and supporting and showing confidence in their work groups. Access to sufficient resources is also necessary for a creative climate, including funds, materials, facilities, and information. In addition, employee perceptions that the work they are doing is challenging and important will also help to cultivate a creative climate. Amabile and colleagues (1996) also found that obstacles such as organizational cultures that impede creativity (e.g., internal politics, harsh criticism of new ideas, avoidance of risk, overemphasizing the status quo) as well as workload pressure (e.g., extreme time pressure, unrealistic expectations productivity) hinder the development of a creative climate. Given all the above, organizations as a whole as well as supervisors need to consider factors if they truly want to set up their employees for success in evaluating novel threats.

**Human Resources Practices**

In addition to leadership, teamwork, and organizational climate, a focus on certain human resources practices can also help overcome a bias against originality. Human resources practices like selecting the right individuals, offering appropriate benefits, appraising performance, managing rewards effectively, and providing the right kinds of training can help to overcome novel threat characteristics, evaluator characteristics, and context characteristics. Each of these will be expanded upon below.

**Selection.**

One key research area within the organizational sciences is understanding how to effectively select personnel. Oftentimes, scholars and practitioners will identify various individual differences that are predictive of relevant performance outcomes. In turn, they can select personnel with specific individual differences that are found to be important for their job. We believe the same can be true for the security workforce in the evaluation of novel threats. Specifically, we believe that taking a selection approach to overcoming a bias against originality may help to address that the emotions of the evaluator may impede the evaluation of novel threats, as well as some of the cognitive challenges that come with a lack of evaluative goals and standards.

Researchers have found that intrinsic motivation for creativity is one of the strongest predictors of employee creativity (Baer et al., 2003; Liu et al., 2016; Malik et al., 2019; van Knippenberg & Hirst, 2020). Finding employees who believe that being creative is inherently satisfying are generally more creative. These same individuals may be better equipped to evaluate novel threats. In addition to intrinsic motivation, creative self-efficacy, an employee being confident in their creative ability, has also been cited as a predictor of creativity (Baer et al., 2003; Liu et al., 2016). Moreover, findings suggest that employees with low scores of agreeableness may improve creative idea evaluation and selection. Although this quality is unrelated to idea generation, disagreeableness can help with originality bias by getting ideas heard and used by others (Cushenbery & Hunter, 2015). Related to teamwork, selecting an employee based on their disagreeableness may improve the team’s creative outcomes. Security personnel who have high levels of these individual differences may be better at evaluating something as fear-inducing and amorphous as a novel threat.
Policies and Resources
The security workforce can strategically hire people with traits that may make them better at evaluating novel threats, but that might not matter if other things within the organization do not allow for creativity. Organizational policies may be able to address the fear-inducing nature of novel threats, the lack of evaluative goals and standards, as well as environmental constraints. For example, de Jonge et al. (2012) found that cognitive resources are related to employee creativity. Specifically, they found that, especially in jobs where cognitive detachment from work was low (e.g., in high-stress jobs), cognitive resources were important for employee creativity. One of these cognitive resources includes opportunities to take breaks when a task requires a lot of concentration. In the security workforce, it may be important to develop policies around limiting overtime or the number of days working in a row to lighten the cognitive load.

This parallels creativity research that posits that leaders need to signal that creativity is desirable for an organization by providing resources for creativity (Hughes et al., 2018; Madjar et al., 2011). For example, we previously discussed the amount of time it would take for evaluators to come up with evaluation criteria with which to judge novel threats. If those working in the security workforce were given dedicated time to tackling this issue, the organization would signal to their organizations that identifying novel threats is desirable. Autonomy is another one of those resources that have been shown to stimulate creativity (Hughes et al., 2018; Liu et al., 2016; Madjar et al., 2011). When possible, purposefully enacting policies that give employees more autonomy should be considered in the security workforce.

Performance Appraisal / Rewards
Most organizations have performance appraisal systems in place where employees are evaluated, given feedback on their performance, and often given raises or promotions for good performance. These appraisals of performance and subsequent rewards for good performance are key to keeping employees motivated. In the security workforce, organizations should create expectations for creativity (van Knippenberg & Hirst, 2020) and signal that creativity is important by making it a job requirement (Kim et al., 2010; Madjar et al., 2011; Shalley et al., 2000; Unsworth et al., 2005). Importantly, if the security workforce wants to reward identifying novel threats, they will need to think carefully about what this means and how to do so in a fair way. Mullin and Sherman (1993, p. 433) posit the following:

“Employees do what management inspects, not what it expects. If management expects creative performance, they must clearly operationalize this value through their performance appraisal system.”

In other words, supervisors can require creativity as part of the job, but unless they actively appraise employee performance based on some operationalization of creative performance, employees will not feel they actually need to perform creatively. In the same vein, supervisors in the security workforce should include the identification of novel threats in the appraisal of employees’ performance. There would also need to be a consideration of the rewards for doing this well. Although there is research to suggest that rewarding creativity is not always a good thing (e.g., Baer et al., 2003; Malik et al., 2019), rewards are not, in and of themselves, bad for creativity (Eisenberger and Armeli, 1997). As such, it will be necessary to think carefully about what specific behaviors will be rewarded and how rewards will be distributed. If performance is being appraised for the evaluation of novel threats and subsequent rewards are being given, acceptance of novelty may become the norm in the security workforce. Given this new “norm”, an additional consequence of rewarding the effective evaluation of novel threats is that these rewards may motivate employees in a way that alleviates some of the social pressures that come with promoting novel ideas.
Training
Finally, requiring training can also help to overcome a bias against originality. Specifically, training can be used as a way to alleviate the difficulties that come with the lack of evaluation standards and goals. Indeed, d’Amato and Hunter (2023) recommend creativity training particularly for the counterterrorism workforce to enhance the detection of novel threats. Specifically, the authors suggest these trainings include not only cognitive skills like how to facilitate creative thinking and action but also how to increase employees’ creative self-efficacy (as discussed in the selection of employees) and how leaders can make changes in their organizations to foster creativity. Similarly, Licuanan et al., (2007) also stress the importance of training to include a focus on enhancing cognitive skills. Specifically, they posit that trainings should encourage employees to frame the evaluation in terms of originality. In other words, employees should be trained to actively look for and analyze ideas with respect to originality. We discussed above the importance of leaders stressing the importance of creativity in the evaluation of novel threats, but alongside this, leaders should support training their employees on exactly how this should be done.

Training may also be able to help overcome barriers related to perceptions of the evaluator. Specifically, Hunter et al. (2022) found that high-quality pitches for highly original ideas may reduce uncertainty in that idea. In the security workforce, if employees are taught how to develop a high-quality pitch for the endorsement of a novel threat, perhaps it will be better received by their peers regardless of previous perceptions. In a similar vein, emotional intelligence training may also be useful in overcoming a bias against originality. Zhou & George (2003) proposed that emotional intelligence will enable leaders to evaluate ideas in an unbiased manner because they will be less likely to dismiss ideas prematurely, accept ideas without constructive and critical assessments, feel threatened, or allow personal relationships to affect perceptions of an idea. Given that emotional intelligence has been characterized as a set of interrelated abilities involved in perceiving, using, understanding, and managing emotions (Lopes et al., 2005; Mayer et al., 2008), it is not surprising that scholars have since discovered that emotional intelligence can be trained (Hodzic et al., 2017). As such, the security workforce may consider implementing emotional intelligence training as one strategy in trying to combat a bias against originality.

Applying Lessons to Future Research Directions
Above we have described how lessons learned in the organizational sciences may benefit the homeland security enterprise in the evaluation of novel threats. Specifically, we were interested in applying these lessons to mitigate a bias against originality. Given that scholars within the organizational sciences have only recently begun to investigate questions related to novel threats (e.g., d’Amato & Hunter, 2023; Hunter & Ligon., 2022; Hunter et al., 2022), there are abundant future research directions in this space. Importantly, we have made many recommendations regarding applying lessons from the organizational sciences to the security workforce. Future research should explore if these recommendations impact the effectiveness of novel threat evaluation (see Table 1).
<table>
<thead>
<tr>
<th>Proposed Explanation for a Bias Against Originality</th>
<th>Lessons Applied</th>
<th>Suggestions for Future Research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perceptions of threat source</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fear inducing quality</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Heuristic access and interpretability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Diversity of expertise</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Emotions</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Novel Threat Characteristics**

- Implement training on developing quality pitches
- Provide cognitive resources (e.g., opportunities to take breaks)
- Cognitive skills trainings for employees

**Evaluator Characteristics**

- Implement training on developing quality pitches
- Foster psychological safety

**Suggested for Future Research**

- Do high-quality explanations of novel threat evaluation ameliorate any perceptions that peers may have of the evaluator?
- Do high-quality pitches impact the credibility of a novel threat?
- What cognitive resources mitigate the effects of fear?
- Can cognitive skills be trained that make the evaluation of fear-inducing threats easier?
- What should be included in the explanation of a novel threat to make it easier to discuss?
- Does psychological safety impact employees’ belief that they can successfully articulate a novel threat?
- What background diversity factors should be considered when composing a threat management team that can effectively evaluate novel threats?
- Are the background diversity factors that increase information exchange in threat assessment teams similar or different from what we have found with other teams?
- Can we select people to evaluate novel threats whose emotions have less of an impact on their evaluation of novel threats? How would applicants perceive this?
- Does having a tolerance of uncertainty improve the evaluation of novel threats?
- Would selecting for tolerance of uncertainty have any backlash effects on organizational performance?
<table>
<thead>
<tr>
<th>Context Characteristics</th>
<th>Accountability pressures</th>
<th>Evaluative goals and standards</th>
<th>Non-Barrier Specific Research Questions</th>
</tr>
</thead>
</table>
| Environmental constraints | Leadership signaling the importance of novelty | Leadership provides intellectual stimulation to encourage innovative thinking | Do lessons learned from traditional organizations apply to the security workforce?  
|                           | Organization signaling the importance of creativity (e.g., performance appraisal and rewards) | Selecting individuals who are better equipped to evaluate novel threats | Which barriers are the most problematic to the effective evaluation of novel threats?  
|                          | Do signals from the organization that it is important to detect novel threats remove pressure? | Provide cognitive resources (e.g., opportunities to take breaks) |  
|                          | Which signals are most effective? | Cognitive skills trainings for employees |  
|                          |                                      | Training leaders on how to increase employee creative self-efficacy |  
|                          |                                      |How effective is training in the evaluation of novel threats? What aspects of training are most important? |  
|                          |                                      |Are there ways to select individuals who are better able to naturally evaluate novel threats? What makes someone better at evaluating novel threats? |  
|                          |                                      |What cognitive skills and resources are most important for evaluating novel threats? |  
|                          |                                      |What resources can be made available to employees to ameliorate environmental constraints to evaluate novel threats? |  
|                          |                                      |Can we train employees on evaluation techniques specifically (i.e., rather than on things like cognitive skills)? What does this look like? |  
|                          |                                      |Does organizational climate impact the evaluation of novel threats? |  
|                          |                                      |How do signals from an organization (i.e., via policies or leadership) that the detection of novel threats is important impact perceptions of organizational climate? |  
|                          |                                      |Do signals from the organization mediate the relationship between climate and evaluation? |  

* * *
SUMMARY STATEMENT AND CONCLUDING COMMENTS

Threat and risk assessment tools play a crucial role in the identification and management of targeted violence, offering key and necessary insights into individuals who are capable and willing to enact violence. Given the importance of such tools, it is not surprising that a range of measures have been developed. The variability of such tools is substantial and has resulted in a measurement landscape that is quite complex. Given the complexity of this area, it was necessary to examine key psychometric issues across the breadth of these tools and provide guidance on their utility.

As such, members of the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, delved into the effectiveness of these methods. This exploration included reviews of extensive literature and interviews with professionals, leading to an encompassing discussion on the efficacy of threat and risk assessment tools, their practical applications, and notable shortcomings in current methodologies.

In addition to a core review of tools, key outputs from this initiative also involved identifying and addressing four major "blind spots" in existing models:

- Overreliance on domestic methods and avoidance of international perspectives.
- Disproportionate focus on federal-level operations without sufficient integration of local practices.
- Neglect of insider threats due to an excessive focus on external risks.
- Ignoring novel threats by concentrating on familiar, frequently occurring dangers.

To help mitigate these issues, the project produced several reports aimed at broadening the scope and understanding of threat assessment:

- A directory of global threat assessment models to encourage the adoption of diverse international methods.
- A focused discussion on lessons from threat assessment practices abroad.
- An examination of local-level practices to enhance federal operations and foster better integration.
- Insights into insider threats to balance the perspective between external and internal risks.
- A critique on the tendency to overlook novel threats, promoting a more comprehensive approach to threat detection.

More broadly, the research emphasized the structured professional judgment (SPJ) tools, highlighting their reliability and adaptability across various scenarios, albeit with varied applications across different teams and contexts. This variability underscores the necessity for ongoing training and the development of a common framework to guide the application of these tools effectively.

The review of SPJ tools revealed training was a significant barrier, with costs and logistical challenges limiting access for many organizations. The research advocated for more affordable and frequent training programs to ensure that practitioners remain proficient and updated in their practices.
Finally, the project stressed the importance of organizational buy-in and interdisciplinary cooperation. Effective threat assessment requires support from all levels of an organization and benefits from diverse perspectives, including IT for insider threats and management for organizational integration.

In conclusion, while threat and risk assessment tools have proven effective, their potential is often undercut by methodological blind spots and operational silos. Addressing these issues through improved training, broader adoption of diverse methods, and enhanced organizational cooperation is essential for advancing the field and effectively mitigating threats.
References


National Counterterrorism, Innovation, Technology, and Education Center (NCITE) (2022b, March). *NCITE briefing on state of science in terrorism and targeted violence prevention efforts.* Briefing memorandum provided to the House Committee on Homeland Security. Omaha, NE.

National Counterterrorism, Innovation, Technology, and Education Center (NCITE) (2022a). *Threat assessment practitioner interviews.* Omaha, NE.


