International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Cyberpsychological Indicators of Mass Violence: Integrating Behavioral Threat Assessment with Law Enforcement Intelligence

Dr. Robb Shawe (Lead Author)
Dr. Robert W. Clark (Co-Author)
Capitol Technology University, Department of Sustainability, Department of Cyber-Psychology, 11301 Springfield Road, Laurel, MD 20708, USA

doi.org/10.51505/ijaemr.2026.11214 URL: http://dx.doi.org/10.51505/ijaemr.2026.11214

Received: Mar 09, 2026 Accepted: Mar 17, 2026 Online Published: Mar 24, 2026

Abstract

Mass violence incidents continue to pose complex challenges for law enforcement agencies and policymakers in the United States. Traditional threat detection models have primarily relied on behavioral observation, investigative intelligence, and reactive response strategies. However, the increasing influence of digital environments on grievance formation, identity reinforcement, and behavioral signaling suggests that cyberpsychological indicators may provide valuable insight into the early stages of violent intent formation. This article examines the intersection of cyberpsychology, behavioral threat assessment, and law enforcement intelligence practices to explore how digital behavioral signals may enhance threat detection capabilities. Drawing upon scholarship examining mass violence, behavioral leakage, and online radicalization dynamics, the study proposes a conceptual framework that integrates cyberpsychological indicators with operational threat assessment models used by law enforcement agencies. The analysis highlights how digital communication patterns, grievance amplification, and identity-driven narratives may function as early indicators of potential violence when interpreted within structured threat assessment frameworks. The findings suggest that integrating cyberpsychological insights with intelligence analysis may enhance prevention strategies, improve situational awareness, and support more proactive public safety approaches. The article concludes by outlining policy implications and directions for future research to strengthen early intervention and violence prevention efforts.

Keywords: cyberpsychology, behavioral threat assessment, mass violence prevention, social media intelligence, law enforcement intelligence

1. Introduction

Mass violence remains one of the most complex and difficult challenges confronting modern law enforcement agencies. While investigative intelligence, community reporting, and behavioral observation have historically formed the basis of threat detection strategies, preventing acts of

Vol. 11, No. 02; 2026

ISSN: 2456-3676

targeted violence continues to present significant analytical difficulties (Borum et al., 1999; Calhoun & Weston, 2015; Fein & Vossekuil, 1998; Fox & Levin, 2015).

Research examining targeted violence has demonstrated that perpetrators frequently display warning behaviors prior to attacks. These behaviors may include fixation on perceived grievances, escalating hostility toward specific individuals or institutions, fascination with previous perpetrators, and communication of violent ideologies (Meloy et al., 2012). Contemporary threat assessment frameworks, therefore, emphasize evaluating patterns of behavior rather than relying on demographic or psychological profiling.

In recent years, the digital environment has become an increasingly significant context for understanding behavioral indicators of violence. Social media platforms and online communication networks allow individuals to express grievances, ideological beliefs, and identity narratives in ways that were not previously observable to investigators. Cyberpsychology research suggests that digital environments may amplify emotional expression, reinforce identity formation, and facilitate the validation of grievance narratives within online communities (Reicher et al., 2008).

Moreover, this article forms part of a broader program of research examining digitally mediated behavioral threats and the evolving analytical frameworks required to identify, interpret, and responsibly govern them. The research program investigates the progression of online behavioral indicators, the mechanisms through which grievance expression may escalate into behavioral leakage, and the role of digital intelligence methods and artificial intelligence–enabled analytics in supporting early threat detection. Complementing these analytical dimensions, the program also explores the ethical and governance considerations necessary to ensure that emerging detection capabilities are implemented responsibly and in alignment with democratic norms and civil liberties. Collectively, this body of work seeks to advance an integrated interdisciplinary framework for understanding and managing digitally mediated threat environments.

A comprehensive understanding of how these cyberpsychological dynamics influence behavioral escalation could significantly enhance law enforcement agencies' capabilities to identify potential threats earlier in the trajectory of violence. By incorporating cyberpsychological indicators into threat assessment frameworks, investigators may acquire further insights into the development of violent intent within digital environments. Furthermore, this article is an integral component of a larger interdisciplinary research initiative that explores cyberpsychological indicators, behavioral leakage pathways, digital intelligence analysis, artificial intelligence–enabled threat detection, and ethical governance frameworks for digitally mediated threat environments.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2. Literature Review

Mass Violence and Behavioral Threat Assessment

Behavioral threat assessment models have emerged as a widely accepted approach for evaluating risks associated with targeted violence. These models focus on identifying patterns of escalating behavior rather than attempting to predict violence based on demographic characteristics (Borum et al., 1999; Calhoun & Weston, 2015; Fein & Vossekuil, 1998; U.S. Secret Service, National Threat Assessment Center, 2019).

Early research conducted by the U.S. Secret Service found that individuals who commit acts of targeted violence often demonstrate observable warning behaviors prior to attacks (Vossekuil et al., 2002). These behaviors may include grievance formation, fixation on violent narratives, and expressions of hostility toward perceived adversaries.

Subsequent research has expanded these findings by identifying patterns of behavioral escalation associated with targeted violence. Analysts are encouraged to examine behavioral trajectories over time, evaluating how psychological stressors, social dynamics, and environmental influences contribute to the progression toward violence (Meloy et al., 2012).

Behavioral Leakage and Pre-Attack Indicators

One of the most important concepts within threat assessment research is **behavioral leakage**, which refers to the communication of violent intent or grievance narratives prior to an attack (Meloy & Gill, 2016; Meloy & O'Toole, 2011; O'Toole, 2000). Leakage may occur through verbal statements, written communications, or digital interactions that reveal elements of an individual's psychological state.

Studies examining active shooter incidents have shown that many perpetrators communicate concerning behaviors or threats before committing acts of violence (Silver et al., 2018). These communications may not always be interpreted as credible threats at the time, but often reveal patterns of escalating grievance narratives.

The increasing prevalence of digital communication platforms has expanded the contexts in which behavioral leakage may occur. Online manifestos, social media posts, and participation in extremist online communities may provide insight into evolving ideological commitments.

Cyberpsychology and Online Behavioral Expression

Cyberpsychology research explores how digital environments influence psychological processes and social behavior. Online platforms can amplify emotional expression, strengthen the formation of group identity, and reinforce ideological narratives through social feedback mechanisms (Postmes et al., 1998; Reicher et al., 2008; Suler, 2004).

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Recent scholarship has further emphasized that digital communication environments may accelerate grievance reinforcement and identity alignment processes through algorithmic amplification and networked audience feedback, thereby intensifying emotional expression and ideological commitment within online communities (Conway, 2017; Gill et al., 2017).

Individuals who express grievances online may experience psychological reinforcement when digital audiences validate their beliefs. This validation can contribute to the escalation of narratives of victimization and perceived injustice.

Digital environments may also facilitate symbolic identification with prior perpetrators of violence. Media coverage and online discourse surrounding mass violence incidents may create contagion effects in which individuals view perpetrators as symbolic figures of recognition or validation (Lankford, 2016; Peterson et al., 2021).

Social Media Contagion and Radicalization

Online communication networks allow violent narratives to spread rapidly across global audiences. Exposure to violent events through digital media may influence behavioral trajectories toward violence by increasing the visibility and symbolic significance of such acts (Lankford, 2016; Nacos, 2007; Towers et al., 2015; Weimann, 2016).

In some cases, individuals who identify with the motivations of previous perpetrators may attempt to emulate their actions. Understanding these contagion pathways is therefore critical for developing prevention strategies that address both psychological and social dynamics within digital environments.

3. Conceptual Framework

Building on the preceding literature examining behavioral threat assessment, cyberpsychological dynamics, and digital behavioral leakage, the following conceptual framework illustrates how online behavioral signals may interact with established threat-assessment models used by law enforcement agencies.

The conceptual framework proposed in this article integrates cyberpsychological indicators with established behavioral threat assessment models. The framework suggests that digital behavioral signals may provide insight into the psychological progression that precedes acts of mass violence.

Three core components are central to this framework:

1. **Grievance Formation** – Individuals develop narratives of perceived injustice or victimization.
2. **Digital Expression and Identity Reinforcement** – Grievances are expressed through online platforms where individuals may receive validation from digital communities.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

3. **Behavioral Leakage and Escalation** – Individuals begin communicating signals that indicate escalating hostility or fascination with violence.

Interpreting these signals within structured threat assessment models may help investigators identify behavioral trajectories associated with potential violence.

4. Methodological Orientation

This study adopts a **conceptual and doctrinal synthesis approach** that integrates scholarship from cyberpsychology, criminology, and threat assessment research in law enforcement. Rather than relying on a single empirical dataset, the analysis synthesizes theoretical frameworks and empirical findings from multiple scholarly domains.

Conceptual synthesis allows researchers to explore relationships between cyberpsychological constructs and operational frameworks used by practitioners. By examining scholarship on grievance formation, behavioral leakage, and digital identity reinforcement, the study develops a conceptual model that may inform threat detection strategies.

Such interdisciplinary approaches are particularly valuable when addressing complex phenomena such as mass violence, which involve interactions among psychological, social, and technological factors (Fox & Levin, 2015; Rocque & Duwe, 2018).

5. Analysis and Discussion

Integrating cyberpsychological insights into threat assessment practices may enhance the early identification of individuals at risk of violence. Traditional models focus on observable behaviors such as threats, fixation on prior attackers, or suspicious weapon acquisitions. However, digital environments often reveal behavioral signals earlier within the escalation process.

Online communication platforms provide environments where grievance narratives can develop and intensify. Individuals may use these platforms to express hostility, ideological beliefs, or emotional distress. When such expressions occur alongside escalating behavioral patterns, they may provide important indicators for threat assessment teams.

In some documented cases, individuals who later committed acts of targeted violence had previously expressed escalating grievance narratives through online posts, forum participation, or symbolic references to prior attackers. Although such communications may not initially appear as explicit threats, they can serve as behavioral-leakage signals that, when evaluated alongside other behavioral indicators, may provide early insights into evolving risk trajectories.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Understanding the psychological dynamics of online communities is, therefore, critical for interpreting digital behavioral signals. Analysts must evaluate how digital expressions interact with offline behaviors and environmental stressors in shaping behavioral trajectories.

6. Policy and Operational Implications

The proposed conceptual model illustrates how cyberpsychological indicators may inform law-enforcement threat-detection systems. The model identifies four interconnected stages that may characterize the progression from grievance formation to potential violent action.

1. **Grievance Formation**
   Individuals develop narratives of injustice or perceived victimization. These grievances may arise from personal conflicts, ideological beliefs, or broader social frustrations.

2. **Digital Expression and Identity Reinforcement**
   Grievances are expressed through digital platforms, where individuals may seek validation from online communities. These interactions may reinforce identity alignment with extremist narratives or violent actors.

3. **Behavioral Leakage and Escalation**
   Individuals begin communicating signals that may indicate escalating hostility or fascination with violence. These signals may appear through threatening language, symbolic references to prior attacks, or increased engagement with violent content.

4. **Operational Threat Indicators**
   Escalation may culminate in behaviors associated with attack preparation, such as reconnaissance, weapon acquisition, or direct threats against specific targets.

When interpreted collectively, these stages provide a framework for integrating cyberpsychological insights into threat assessment processes. The model emphasizes the importance of analyzing **behavioral patterns over time**, rather than relying on isolated digital statements. To operationalize the integration of cyberpsychological indicators with structured threat-assessment practices, the following conceptual model illustrates how digital behavioral signals align with staged threat-detection processes within law enforcement intelligence frameworks. The conceptual model presented in Figure 1 illustrates how cyberpsychological indicators may emerge across stages of grievance formation, digital expression, and behavioral escalation utilized within digital environments.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Integrated Cyberpsychological Threat Assessment Model

Note. Author created. The conceptual model illustrates the progression from grievance formation to operational threat indicators through cyberpsychological processes expressed within digital environments. The framework highlights how behavioral signals communicated through online platforms may inform structured threat assessment processes used by law enforcement agencies.

Taken together, the model demonstrates that cyberpsychological indicators, when interpreted within structured threat assessment frameworks, provide a critical linkage between early-stage digital behavioral expression and operational threat identification, thereby enhancing the capacity of law enforcement to detect and intervene in emerging violence trajectories.

7. Limitations and Future Research

This study adopts a conceptual synthesis approach rather than empirical analysis. While this approach enables theoretical integration across multiple disciplines, the proposed framework has not yet been tested using large-scale datasets.

Future research should examine cyberpsychological indicators through empirical methods such as case-based analysis, digital behavioral pattern analysis, and network analysis of online extremist communities. Integrating computational social science methods with threat assessment research may improve the predictive capabilities of violence prevention frameworks.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

8. Conclusion

Preventing mass violence requires a deeper understanding of the behavioral trajectories that precede acts of violence. Beyond its applied implications, this study contributes to the theoretical development of cyberpsychological threat assessment by integrating digital behavioral signaling with established models of behavioral escalation, thereby advancing a governance-informed framework for interpreting digitally mediated indicators of targeted violence. While traditional threat assessment models provide valuable insights, the increasing influence of digital environments necessitates expanded analytical frameworks.

Cyberpsychological research offers valuable insight into how grievance narratives, identity reinforcement, and behavioral signaling develop within online communities. Integrating these insights into threat assessment practices may improve early identification of potential violence and strengthen prevention strategies.

Authorship Statement

Dr. Robb Shawe and Dr. Robert W. Clark jointly conceptualized the research framework and analytical orientation of this manuscript. Dr. Clark contributed practitioner expertise derived from federal law enforcement leadership and public safety governance experience. Dr. Shawe contributed a scholarly synthesis across cyberpsychology, critical infrastructure protection, and public safety governance, including the integration of literature and manuscript preparation. Both authors reviewed and approved the final manuscript.

Author Note and Copyright Statement

Dr. Robb Shawe, PhD, is a scholar-practitioner, U.S. Navy veteran, and Chief Executive Officer of New York Security Consulting Professionals L.L.C. His research focuses on critical infrastructure protection, cybersecurity governance, and resilience systems. Dr. Shawe served as the lead author and was primarily responsible for conceptualization, development of the analytical framework, and manuscript preparation.

Dr. Robert W. Clark, PhD, currently serves as Deputy Mayor of Public Safety for the City of Los Angeles and previously served as an Assistant Special Agent in Charge with the Federal Bureau of Investigation. His research focuses on mass violence prevention, behavioral threat assessment, and the intersection of cyberpsychology and public safety intelligence. Dr. Clark contributed to the literature synthesis, conceptual refinement, and collaborative development of the research framework. Both authors participated in reviewing and approving the final version of the manuscript.

The authors declare no conflicts of interest related to this research. The manuscript represents original scholarly work and is not currently under consideration by another publication outlet.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

References

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences & the Law, 17*(3), 323–337.

Calhoun, F. S., & Weston, S. W. (2015). *Threat assessment and management strategies: Identifying the howlers and hunters*. CRC Press.

Citron, D. K., & Gray, D. (2013). Addressing the harm of total surveillance: A reply to Professor Neil Richards. *Harvard Law Review Forum, 126*, 262–272.

Clark, R. W. (2025). *Mass shootings in America: A law enforcement response* (Unpublished doctoral dissertation). Capitol Technology University.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77–98.

Fein, R. A., & Vossekuil, B. (1998). Preventing assassination: The Secret Service exceptional case study project. *Annals of the American Academy of Political and Social Science, 576*(1), 62–74.

Fox, J. A., & Levin, J. (2015). *Extreme killing: Understanding serial and mass murder* (3rd ed.). Sage.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy, 16*(1), 99–117.

Gill, P., Horgan, J., & Deckert, P. (2014). Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. *Journal of Forensic Sciences, 59*(2), 425–435.

Innes, M., Fielding, N., & Cope, N. (2005). The appliance of science? The theory and practice of crime intelligence analysis. *British Journal of Criminology, 45*(1), 39–57.

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the internet. *Journal for Deradicalization, 1*, 116–134.

Lankford, A. (2016). *Public mass shooters and firearms: A cross-national study of 171 countries.* Violence and Victims, 31(2), 187–199.

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

Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law, 29*(4), 513–527.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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

Nacos, B. L. (2007). *Mass-mediated terrorism: The central role of the media in terrorism and counterterrorism* (2nd ed.). Rowman & Littlefield.

O'Toole, M. E. (2000). The school shooter: A threat assessment perspective. *FBI Law Enforcement Bulletin, 69*(10), 7–10.

Peterson, J., Densley, J., & Erickson, A. (2021). *The violence project: How to stop a mass shooting epidemic*. Abrams Press.

Postmes, T., Spears, R., & Lea, M. (1998). Breaching or building social boundaries? SIDE-effects of computer-mediated communication. *Communication Research, 25*(6), 689–715.

Ratcliffe, J. H. (2016). *Intelligence-led policing* (2nd ed.). Routledge.

Reicher, S., Spears, R., & Postmes, T. (2008). A social identity model of deindividuation phenomena. *European Review of Social Psychology, 6*(1), 161–198.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934–1965.

Rocque, M., & Duwe, G. (2018). The patterns and correlates of mass murder in the United States. *Homicide Studies, 22*(2), 131–155.

Shawe, R. (2025). *Exploring smart grid technologies' impact on sustainable energy management in New York State* (Publication No. 32284053) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations & Theses Global.

Silver, J., Simons, A., & Craun, S. (2018). *A study of the pre-attack behaviors of active shooters in the United States between 2000 and 2013*. Federal Bureau of Investigation.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, 7*(3), 321–326.

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 33–47). Brooks/Cole.

Towers, S., Gomez-Lievano, A., Khan, M., Mubayi, A., & Castillo-Chavez, C. (2015). Contagion in mass killings and school shootings. *PLoS ONE, 10*(7), e0117259.

U.S. Secret Service, National Threat Assessment Center. (2018). *Enhancing school safety using a threat assessment model: An operational guide for preventing targeted school violence*. U.S. Department of Homeland Security.

U.S. Secret Service, National Threat Assessment Center. (2019). *Protecting America's schools: A U.S. Secret Service analysis of targeted school violence*. U.S. Department of Homeland Security.

Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The final report and findings of the Safe School Initiative*. U.S. Secret Service and U.S. Department of Education.

Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.