International Journal of Advanced Engineering and Management Research

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Cyberpsychological Indicators and Digital Pathways to Targeted Violence: A Behavioral Leakage and Online Radicalization Model

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.2026.11213 URL: http://dx.doi.org/10.51505/ijaemr.2026.11213

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

Abstract
Understanding the behavioral pathways that precede targeted violence remains a central challenge for threat assessment professionals and researchers. Increasingly, these pathways develop within digital environments where identity formation, grievance amplification, and behavioral signaling occur publicly. This study synthesizes threat assessment scholarship, cyberpsychology research, and radicalization studies to examine how online environments facilitate behavioral leakage and escalation toward targeted violence. Drawing on established models of warning behaviors, social identity dynamics, and online disinhibition, the article proposes a conceptual framework describing how digital interactions may contribute to the progression from grievance development to observable threat indicators. The framework highlights the interaction between psychological factors, online group dynamics, and behavioral signaling processes. Implications are discussed for threat assessment practitioners, law enforcement, and researchers seeking to identify early indicators of risk within digital ecosystems.

Keywords: cyberpsychology, targeted violence, behavioral leakage, online radicalization, threat assessment

1. Introduction

Building on prior research on cyberpsychological indicators of mass violence, this article investigates the behavioral pathways through which the digital expression of grievances may develop into behavioral leakage and observable threat indicators. Threat assessment research has consistently shown that acts of targeted violence are seldom spontaneous and are often preceded by detectable behavioral cues (Borum et al., 1999; Fein & Vossekuil, 1998; Meloy et al., 2012). Individuals who commit violent acts frequently exhibit warning behaviors, communicate grievances, or reveal their intentions prior to an attack (Meloy & O'Toole, 2011; Silver et al., 2018). In modern society, many of these signals increasingly manifest within digital

Vol. 11, No. 02; 2026

ISSN: 2456-3676

environments where communication patterns, ideological reinforcement, and identity construction occur through online platforms.

The rapid expansion of social media and digital communities has transformed how grievances are expressed and amplified. Online spaces may facilitate identity reinforcement, echo-chamber effects, and exposure to extremist narratives, potentially accelerating pathways toward radicalization or violence (Conway, 2017; Koehler, 2014; Weimann, 2016). At the same time, these environments provide opportunities for behavioral leakage, allowing individuals to reveal intentions, fantasies, or escalating grievances in publicly observable ways.

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.

Despite the increasing convergence of digital behavior and threat assessment, there exists a limited number of conceptual frameworks that integrate cyberpsychology research with established models of warning behaviors and targeted violence. This article addresses that gap by synthesizing interdisciplinary literature and proposing a conceptual model that elucidates how cyberpsychological dynamics facilitate behavioral leakage and escalation toward violence. Moreover, the article contributes to a broader interdisciplinary research initiative that investigates cyberpsychological indicators, pathways of behavioral leakage, digital intelligence analysis, threat detection enabled by artificial intelligence, and ethical governance frameworks for digitally mediated threat environments.

2. Literature Review

2.1 Threat Assessment and Targeted Violence

Threat assessment frameworks emphasize the importance of identifying warning behaviors that may precede acts of targeted violence (Borum et al., 1999; Fein & Vossekuil, 1998). Research conducted through the U.S. Secret Service Safe School Initiative and related studies demonstrates that perpetrators often display observable behavioral patterns prior to attacks (Vossekuil et al., 2002).

Subsequent scholarship expanded these insights by identifying specific behavioral indicators associated with escalating risk. Meloy et al. (2012) introduced a typology of warning behaviors,

Vol. 11, No. 02; 2026

ISSN: 2456-3676

including fixation, identification, leakage, and pathway behaviors. These indicators provide a structured framework for evaluating potential threats and understanding how individuals progress from grievance to action.

Mass violence research similarly emphasizes the importance of behavioral precursors. Studies examining active shooter incidents have found that many perpetrators communicated grievances, expressed violent ideation, or demonstrated escalating behaviors prior to attacks (Silver et al., 2018; Rocque & Duwe, 2018).

2.2 Behavioral Leakage and Pre-Attack Indicators

Behavioral leakage refers to the communication of intent to harm prior to an act of violence (Meloy & O'Toole, 2011). Leakage may occur through verbal statements, written communication, or digital expression. In many cases, these signals are observable by peers, family members, or members of online communities.

Research examining pre-attack behaviors suggests that leakage occurs in a substantial proportion of targeted violence cases (Silver et al., 2018). These signals may include statements of grievance, fascination with violence, or explicit threats communicated through interpersonal or digital channels.

The presence of leakage does not necessarily indicate imminent violence; however, it represents an important behavioral signal that may assist threat assessment professionals in identifying individuals at elevated risk.

2.3 Cyberpsychology and Online Behavior

Cyberpsychology research provides insight into how individuals behave within digital environments. One of the most widely cited phenomena is the **online disinhibition effect**, which describes how anonymity and reduced social cues may encourage individuals to express thoughts or behaviors they would not display in offline settings (Suler, 2004).

Digital communication also influences group dynamics and identity formation. Social identity theory suggests that individuals derive a sense of identity and belonging from group membership (Tajfel & Turner, 1979). Online environments may intensify these processes by facilitating interaction within ideologically homogeneous communities.

Research examining computer-mediated communication further suggests that online interaction may strengthen group polarization and reinforce shared beliefs (Postmes et al., 1998; Reicher et al., 2008). These dynamics can amplify grievances and reinforce ideology within digital networks.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

2.4 Online Radicalization and Digital Extremism

The internet has become a significant platform for ideological dissemination and radicalization. Studies examining extremist movements demonstrate that digital environments provide opportunities for recruitment, the dissemination of propaganda, and ideological reinforcement (Conway, 2017; Koehler, 2014).

Research also suggests that online communities may normalize extreme beliefs and reinforce grievance narratives (Weimann, 2016). In some cases, individuals may become increasingly isolated from alternative perspectives as they engage with ideologically aligned networks.
Although most individuals exposed to extremist content do not engage in violence, these environments may facilitate the development of grievance narratives and identity reinforcement that contribute to radicalization pathways.

3. Conceptual Model

The literature reviewed above suggests that cyberpsychological dynamics, behavioral leakage, and threat assessment indicators interact within digital environments. Building on this research, the present study proposes a conceptual framework describing how online behavior may contribute to the escalation of targeted violence risk.

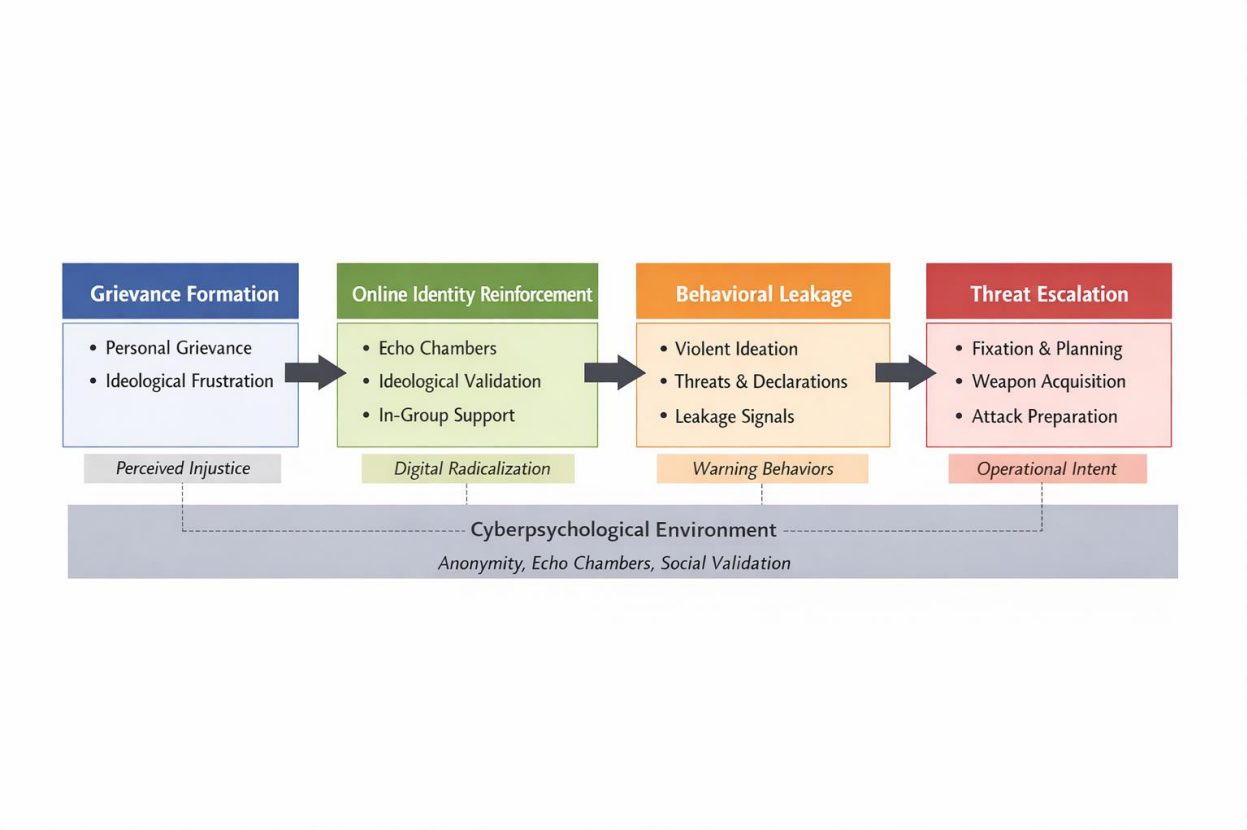
To synthesize these interdisciplinary insights and clarify the progression from digital grievance expression to observable threat indicators, a conceptual model is proposed to illustrate how cyberpsychological dynamics, online interaction patterns, and behavioral leakage converge within digitally mediated environments. Figure 1 illustrates the proposed cyberpsychological pathway through which grievance formation, digital identity reinforcement, and behavioral leakage may lead to observable threat-escalation behaviors.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

Figure 1

Cyberpsychological Pathways to Behavioral Leakage and Targeted Violence



Note. Author created. The model illustrates the interactions among grievance formation, online identity reinforcement, behavioral leakage, and threat escalation in digital environments.

Taken together, the model demonstrates that pathways to targeted violence in digital environments are shaped by the interaction of psychological vulnerability, online identity reinforcement, and observable behavioral leakage, reinforcing the need for integrated analytical frameworks that combine cyberpsychological insight with structured threat assessment methodologies.

4. Implications for Threat Assessment

Understanding how cyberpsychological dynamics influence behavioral leakage has important implications for threat assessment professionals. Digital environments increasingly function as spaces where grievances are expressed, identities are reinforced, and warning behaviors emerge. Threat assessment practitioners may benefit from incorporating digital behavioral indicators into risk evaluation processes. Monitoring patterns of online communication, ideological

Vol. 11, No. 02; 2026

ISSN: 2456-3676

reinforcement, and behavioral signaling may provide additional insight into the escalation of threat trajectories. Such indicators may include repeated grievance articulation, symbolic identification with prior perpetrators, escalation in hostile language, and increased engagement with extremist or violence-related content within digital communities.

The integration of cyberpsychological indicators into threat assessment practices also raises important ethical and governance considerations. The monitoring and interpretation of digital behavioral signals must be carefully balanced with privacy protections, civil liberties, and the risk of false-positive identification. Without appropriate governance safeguards, there is a risk of over-surveillance or misinterpretation of online expression. Accordingly, the development of cyberpsychological threat detection capabilities should be accompanied by clear ethical guidelines, oversight mechanisms, and accountability structures to ensure responsible and proportionate use.

5. Limitations and Future Research

This study presents a conceptual synthesis of existing literature rather than an empirical analysis. Future research should examine digital behavioral patterns using mixed-method approaches, including case studies, social media analysis, and behavioral data.

The literature included in this analysis was selected based on its relevance to behavioral threat assessment, cyberpsychology, and online radicalization processes, with particular emphasis on peer-reviewed studies and government-supported research examining pre-attack behaviors and digital communication dynamics. Sources were analyzed using a thematic synthesis approach to identify recurring constructs related to grievance formation, behavioral leakage, and identity reinforcement across both offline and digital environments.

Further investigation is also needed to examine how specific online environments influence the formation of grievances, identity reinforcement, and behavioral leakage.

6. Conclusion

The intersection of cyberpsychology, threat assessment, and digital communication represents an increasingly important area of research. Online environments provide spaces for grievances to be expressed, identities to be reinforced, and behavioral signals to be communicated.

By integrating insights from threat assessment scholarship and cyberpsychology research, this article proposes a conceptual framework that describes how digital behavior may contribute to pathways to targeted violence. Continued research in this area may help practitioners and policymakers identify early-warning indicators and develop governance frameworks that balance proactive threat detection with civil liberties and democratic oversight.

Vol. 11, No. 02; 2026

ISSN: 2456-3676

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. Copyright will remain with the authors unless transferred to a publisher upon acceptance for publication.

Copyright Notice

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.

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. *Studies in Conflict & Terrorism, 40*(1), 77–98.

Fein, R. A., & Vossekuil, B. (1998). Preventing assassination. *Annals of the American Academy of Political and Social Science, 576*(1), 62–74.

Koehler, D. (2014). The radical online. *Journal for Deradicalization, 1*, 116–134.

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

Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). Warning behaviors in threat assessment. *Behavioral Sciences & the Law, 30*(3), 256–279.

Postmes, T., Spears, R., & Lea, M. (1998). Breaching or building social boundaries? *Communication Research, 25*(6), 689–715.

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

Rocque, M., & Duwe, G. (2018). The patterns and correlates of mass murder. *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*. FBI.

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 *The social psychology of intergroup relations*.

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

Weimann, G. (2016). *Terrorism in cyberspace*. Columbia University Press.