

ADOLESCENTS, DISINFORMATION, AND AI PROFILING: A FORENSIC CYBERPSYCHOLOGY APPROACH TO MITIGATING NATIONAL SECURITY RISKS

Francis C. OHU
fohu@captechu.edu

Laura A. JONES
lajones@captechu.edu
CAPITOL TECHNOLOGY UNIVERSITY, LAUREL, MD, USA

ABSTRACT

Adolescents are increasingly immersed in AI-curated digital environments that amplify disinformation, heightening susceptibility to psychological manipulation with profound implications for mental health and national security. This perspective paper examines how forensic cyberpsychology and AI profiling can be applied ethically to identify adolescents at risk of engaging with disinformation. Drawing on a thematic synthesis of recent studies, the paper identifies vulnerability markers, including validation-seeking, peer conformity, and identity confusion, and explains how these are reinforced through algorithmic amplification. A conceptual framework is proposed to guide the ethical use of forensic AI profiling and targeted interventions. By reframing adolescent disinformation susceptibility as both a developmental and algorithmic risk, this paper emphasizes the need to integrate ethical AI, media literacy, and national security perspectives into a unified prevention strategy.

KEYWORDS:

forensic cyberpsychology, adolescent disinformation, algorithmic amplification, ethical AI, national security

1. Introduction

Digital platforms such as TikTok, Instagram, and Snapchat dominate adolescent information environments, offering unprecedented opportunities for connection while exposing youth to high volumes of misinformation (Owens, 2024; Shin & Jitkajornwanich, 2024). Research shows that most adolescents in the United States encounter conspiracy theories weekly, and a majority believe at least one (Byrne et al., 2024). This vulnerability is exacerbated by AI algorithms that curate emotionally charged and ideologically biased content,

creating echo chambers and reinforcing cognitive biases. The developmental stage of adolescence, marked by identity formation and heightened peer influence, compounds these risks (Szabó et al., 2024). Adolescents, therefore, occupy a dual role as both targets and amplifiers of disinformation, creating profound implications for civic trust and national security. Addressing this problem requires interdisciplinary insights that bring together forensic cyberpsychology, developmental psychology, and AI ethics (Ohu & Jones, 2025b).

2. Problem Statement and Purpose

The widespread dissemination of disinformation among adolescents, facilitated by AI-driven content curation on social media platforms, poses significant risks to national security (Ohu & Jones, 2025). The consequences of this phenomenon are multifaceted, including the erosion of civic trust, the amplification of social divisions, and the potential for radicalization. Furthermore, the vulnerability of adolescents to disinformation threatens their ability to form informed opinions, make critical decisions, and engage in constructive civic participation. This problem statement underscores the urgent need for a comprehensive approach to mitigate the risks associated with adolescent disinformation and AI profiling.

The purpose of this paper is to propose a forensic cyberpsychology approach to understanding the intersection of adolescent vulnerability, disinformation, and AI profiling. Specifically, this study aims to examine the psychological and developmental factors that contribute to adolescent susceptibility to disinformation, investigate the role of AI-driven content curation in amplifying disinformation and validation-seeking behaviors, and explore the potential of forensic AI profiling as a tool for detecting risk factors while respecting ethical boundaries. By achieving these objectives, this study seeks to provide a conceptual roadmap for prevention and early intervention, ultimately informing strategies to mitigate the risks associated with adolescent disinformation and AI profiling.

3. Significance, Originality, and Rationale of the Inquiry

This study is significant as it reframes forensic inquiry for the digital age by situating adolescent disinformation susceptibility at the nexus of psychology, technology, and security. This paper advances the field of Forensic cyberpsychology by showing how digital

environments function as risk ecosystems, amplifying adolescents' developmental vulnerabilities, such as impulsiveness, identity instability, and validation-seeking, through algorithmic curation (Ohu & Jones, 2025d). Hostile actors strategically exploit these vulnerabilities, creating risks that extend beyond individual well-being into civic trust and national security. By recognizing these vulnerabilities as both psychological and algorithmic in origin, the study expands forensic science to include proactive, systemic interventions designed to safeguard cognitive and emotional integrity. The originality of this inquiry lies in integrating adolescent psychology, algorithmic amplification, and forensic profiling into a unified conceptual framework, positioning forensic cyberpsychology as a discipline capable of informing preventive design, ethical governance, and developmental safeguards (Ohu & Jones, 2025a), and reimagining the role of forensic science as a critical contributor to public policy, technological accountability, and the protection of vulnerable populations. This expanded lens demonstrates how forensic cyberpsychology can be leveraged not only to understand the impacts of technology but also to shape its responsible application, ensuring that innovations serve human well-being and democratic stability.

4. Literature Synthesis

This perspective paper is based on a structured narrative synthesis of peer-reviewed studies published between 2020 and 2025. Using databases such as Google Scholar, PsycINFO, Scopus, and PubMed, studies were screened for relevance to adolescent disinformation susceptibility, AI profiling, and forensic cyberpsychology. Forty-seven studies were thematically analyzed using Braun and Clarke's framework (2024), as shown in Figure no. 1. The synthesis emphasizes patterns across psychological vulnerabilities, algorithmic amplification, and preventive interventions. While this is not primary empirical

research, the strength of this approach lies in integrating interdisciplinary insights into a forward-looking conceptual framework.

5. A Forensic Cyberpsychology Approach

Forensic cyberpsychology is an emerging interdisciplinary domain examining how digital technologies, including social media platforms, algorithms, and AI-generated content, intersect with psychological vulnerabilities to influence behavior in contexts relevant to justice, security, and cyber operations (Ohu & Jones, 2025b). This approach scrutinizes how algorithmic manipulation and identity-based targeting mirror psychological operations seen in cyber warfare, exploiting adolescents' cognitive and emotional susceptibilities. By analyzing strategies common to disinformation campaigns, such as repeated exposure to emotionally evocative narratives or algorithm-driven echo chambers, through a forensic lens, researchers can understand how they create behavioral patterns, influence judgment, and can be detected or mitigated in intelligence and security contexts (Ohu & Jones, 2025a).

– National Security Risks

Adolescent-targeted disinformation and AI-generated content create multiple layers of threat to national security, including deepfake-based manipulation, disinformation supply chain proliferation, and AI-amplified social engineering and radicalization. Hyper-realistic deepfakes can be weaponized to fabricate evidence, falsify surveillance footage, or impersonate authorities, eroding trust in legitimate institutions and disrupting intelligence operations, thereby challenging the veracity of visual records and obstructing national security apparatuses from relying on authentic data streams. The easy accessibility of generative AI tools enables a rapidly expanding deepfake supply chain, generating disinformation at scale, automating, and disseminating it widely (Romanishyn et al., 2025; Saha et al., 2024), compromising

individual liberties, manipulating electoral processes, or destabilizing public trust in government institutions. Furthermore, generative models pose risks of facilitating large-scale radicalization or extremist recruitment, particularly among adolescents, who are vulnerable to AI-crafted persuasive narratives, raising concerns over ideologically motivated influence campaigns, and necessitating legislative and technological interventions to address the content and its origins across the supply chain, as well as policy, education, and technical safeguards to mitigate these threats.

– Psychological Vulnerability

Studies consistently identify peer conformity, identity confusion, and digital validation-seeking as predictors of misinformation susceptibility among adolescents. Adolescents high in social comparison behaviors are more likely to share ideologically charged content, often as a means of gaining recognition or belonging (Ohu & Jones, 2025d). These psychological vulnerabilities are reinforced when digital platforms provide positive feedback for engagement, even when the content is harmful. This forensic lens underscores that these traits not only shape digital risk but also offer markers for profiling and prevention.

– Algorithmic Amplification

AI-curated systems optimize for engagement, which often means prioritizing emotionally charged and ideologically polarized content. Research indicates that such algorithms create echo chambers where adolescents repeatedly encounter the same narratives, deepening their susceptibility (Burrell, 2024; Ohu & Jones, 2025d). The role of algorithmic reinforcement in adolescent disinformation engagement is one of the strongest findings across recent literature. This amplification effect mirrors psychological operations strategies traditionally associated with information warfare, underscoring the national security implications of adolescent vulnerability (Ohu & Jones, 2025b).

– ***Cognitive Identity Struggles***

Adolescents are navigating identity formation, and algorithmic personalization often feeds into this process by promoting content that aligns with or exploits their identity struggles. This creates an increased risk of confusion, polarization, and vulnerability to manipulative narratives disguised as activism or a sense of belonging. Studies have linked identity distress to higher rates of impulsive content sharing, further demonstrating how developmental challenges intersect with digital manipulation (Pérez-Torres, 2024).

– ***Ethical AI Profiling and Moderation***

While AI tools can detect behavioral and psychological markers, most current systems are modeled on adult populations and fail to account for adolescent developmental specificity. Ethical profiling requires context-sensitive tools that include adolescent-informed consent, safeguards for mental health, and transparency in the use of data (Chng et al., 2025). Emerging work suggests that adaptive AI systems that integrate emotional tone and peer dynamics can reduce false positives and support trauma-informed interventions.

– ***Parental Mediation and Educational Interventions***

Parental engagement and school-based programs play a critical role in building resilience. Adolescents with active parental mediation are less likely to accept manipulative content uncritically, and digital literacy programs have demonstrated improvements in critical evaluation skills (Ohu & Jones, 2025c). However, restrictive strategies may reduce autonomy, making balanced approaches essential. Integrating AI-driven monitoring with transparent, participatory frameworks can enhance trust and effectiveness.

6. Theoretical Lens and Key Insights

6.1. Erikson Psychosocial Development Theory

Adolescent susceptibility to disinformation is strongly predicted by well-established psychological markers, including identity confusion, peer conformity, and validation-seeking, which are accentuated during this critical developmental window. According to Erikson's Psychosocial Development Theory, particularly the stage of Identity vs. Role Confusion, adolescents are engaged in active identity construction, making them especially sensitive to narratives that provide meaning, belonging, and certainty (Raufelder et al., 2021; Murad, 2024). As a result, disinformation campaigns exploit this developmental stage by offering emotionally charged, black-and-white ideologies that simplify complex realities and provide ready-made social scripts.

6.2. Social Identity and Learning Theories

Peer influence significantly intensifies adolescent vulnerability to disinformation. According to Social Identity Theory, adolescents derive substantial self-worth from group affiliation, which can lead to ingroup favoritism and outgroup bias. This cognitive shortcut is strategically manipulated by disinformation actors to polarize youth. Furthermore, online echo chambers that reinforce peer-endorsed content amplify conformity pressure, reducing critical evaluation and increasing susceptibility to ideologically extreme messages. This phenomenon is also supported by Bandura's Social Learning Theory, which highlights the role of observational learning, particularly from influential peer figures or popular online personas, in driving the imitation of disinformation-fueled attitudes and behaviors (Amsari et al., 2024).

6.3. Dual Process Theory of Cognition

Algorithmic amplification plays a significant role as a force multiplier for adolescent psychological vulnerabilities, as recommendation systems, designed to maximize engagement, disproportionately promote content that triggers emotional arousal, such as outrage, fear, or belonging. This phenomenon aligns with Dual-Process Theories of Cognition, including Kahneman's System 1 and System 2 model (Li et al., 2025; Zucchelli et al., 2025). Due to their underdeveloped prefrontal cortex and heightened limbic system activation, adolescents are more likely to engage in impulsive, emotionally driven "System1" thinking (Brassil et al., 2024; Lemaire et al., 2025). Consequently, emotionally resonant disinformation is not only more attractive to adolescent users but also algorithmically rewarded, creating ideological feedback loops that reinforce distorted worldviews over time.

6.4. Cognitive Behavioral Theory

The integration of preventive moderation and ethical profiling strategies offers a promising approach to mitigating disinformation risks among adolescents, grounded in adolescent developmental psychology. Interventions informed by Cognitive Behavioral Theory (CBT) principles can help adolescents reshape maladaptive thinking patterns, promoting critical reflection and emotional regulation when encountering provocative content (Sørensen et al., 2025). Additionally, school and community-based programs, designed with a developmentally appropriate focus, can equip adolescents with essential

metacognitive tools, enabling them to critically evaluate sources, recognize manipulation, and resist social pressure.

6.5. Constructivist Learning Theory

To support adolescents in today's digital ecosystem, it's crucial to implement effective strategies that promote healthy development and protect their rights. One approach is to integrate scaffolded digital literacy curricula that draw on Constructivist Learning Theory, as proposed by Piaget and Vygotsky, in 1972 (Park et al., 2025; Rai, 2025). By incorporating elements from this theory, curricula can foster active learning environments. In these environments, adolescents can build understanding through hands-on exploration, engaging in discussions, and reflecting on their experiences. In conjunction with digital literacy, ethical AI profiling can serve as a valuable tool. When designed with key principles such as transparency, explainability, and consent in mind, AI profiling can also help platforms identify patterns of behavior that may indicate risk. This can be achieved without resorting to pathologizing language or infringing on user autonomy. However, the implementation of these strategies must be approached with caution. It's essential to include safeguards that respect adolescents' rights and psychological agency. This means steering clear of punitive or overly surveillant models that could erode trust. By finding this balance, we can create supportive digital environments that empower adolescents to navigate the online world safely and confidently.

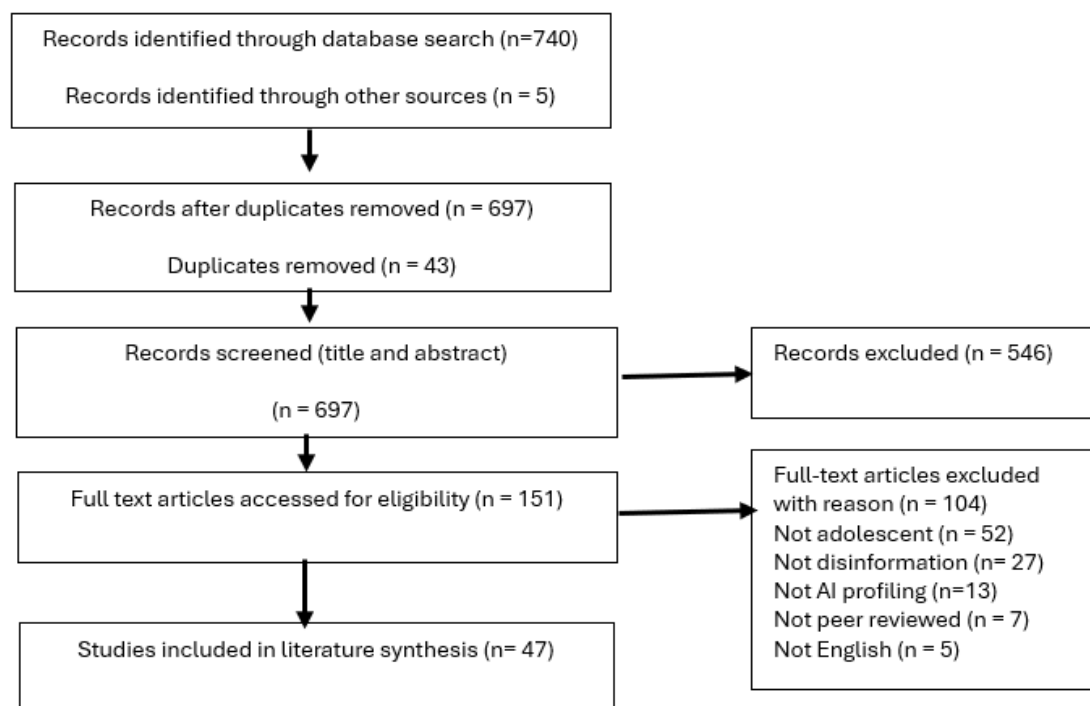


Figure no. 1: *PRISMA Flow Diagram for Literature Synthesis [n = 47]*
(Source: Created by authors)

7. Discussion and Implications

This paper advances the field of forensic cyberpsychology by reconceptualizing adolescent vulnerability to disinformation as a critical intersection of neurodevelopmental immaturity, psychosocial identity formation, and algorithmically driven content curation (Crone & van Drunen, 2024). Rather than viewing adolescents merely as passive consumers of misinformation, this perspective underscores their cognitive, emotional, and social malleability, which adversarial actors exploit using targeted AI-driven profiling. This forensic lens enables a more granular analysis of behavioral patterns, risk typologies, and susceptibilities, forming the basis for intervention strategies that are both preventative and diagnostic in nature. The discussion on ethical AI and adolescent profiling emphasizes the urgent need for algorithmic transparency and age-sensitive design principles. Profiling technologies, often opaque and commercially motivated, must be critically evaluated for their potential to reinforce confirmation biases, polarize identity development, and

manipulate attention in adolescents. Ethical AI frameworks should explicitly address the developmental rights of minors, balancing the necessity of predictive profiling for safety with safeguards that preserve autonomy, informed consent, and psychological integrity. AI systems interacting with youth should be built around explainability, auditability, and opt-in consent mechanisms tailored to varying maturity levels, reflecting not only ethical imperatives but also human rights principles (Ohu & Jones, 2025c).

From a policy and national security standpoint, adolescents are increasingly situated at the frontlines of cognitive security threats. Hostile actors target them not only to influence individual beliefs but also to create long-term sociopolitical destabilization through cumulative psychological manipulation (Ohu & Jones, 2025b). National security frameworks must therefore expand to include digital youth protection protocols as core components of cognitive defense. This includes cross-sectoral collaboration between intelligence

agencies, educational institutions, tech companies, and child welfare organizations. Policy should mandate platform accountability for content amplification mechanisms, particularly those that propagate conspiratorial, extremist, or divisive narratives. Furthermore, legal frameworks should support the development of AI auditing mechanisms and minimum standards for adolescent data governance, situating digital child safety within a broader doctrine of information sovereignty (Ohu & Jones, 2025d).

The implications for educational and parental mediation are equally significant. As algorithmic systems increasingly mediate adolescent attention, identity, and relationships, both schools and families must be empowered to function as proactive buffers. Educational systems must integrate critical digital literacy, cyber psychological resilience, and ethical reasoning into their curricula, not as supplemental topics but as foundational competencies for digital citizenship (Ohu & Jones, 2025c). Media

literacy programs should evolve beyond fact-checking to include skills in recognizing algorithmic manipulation, emotional reasoning, and social engineering tactics. Parental mediation, meanwhile, must move beyond restrictive monitoring toward participatory dialogue, fostering a home environment that supports open discussion about online experiences, encourages reflective thinking, and develops emotional literacy in digital contexts. In summary, mitigating the disinformation threat to adolescents demands a multi-layered strategy grounded in forensic cyberpsychology, steered by ethical AI design, implemented through responsive public policy, and supported by robust educational and familial frameworks. These dimensions must function in unison to safeguard not only individual psychological well-being but also the broader integrity of democratic and national security systems in the algorithmic age.

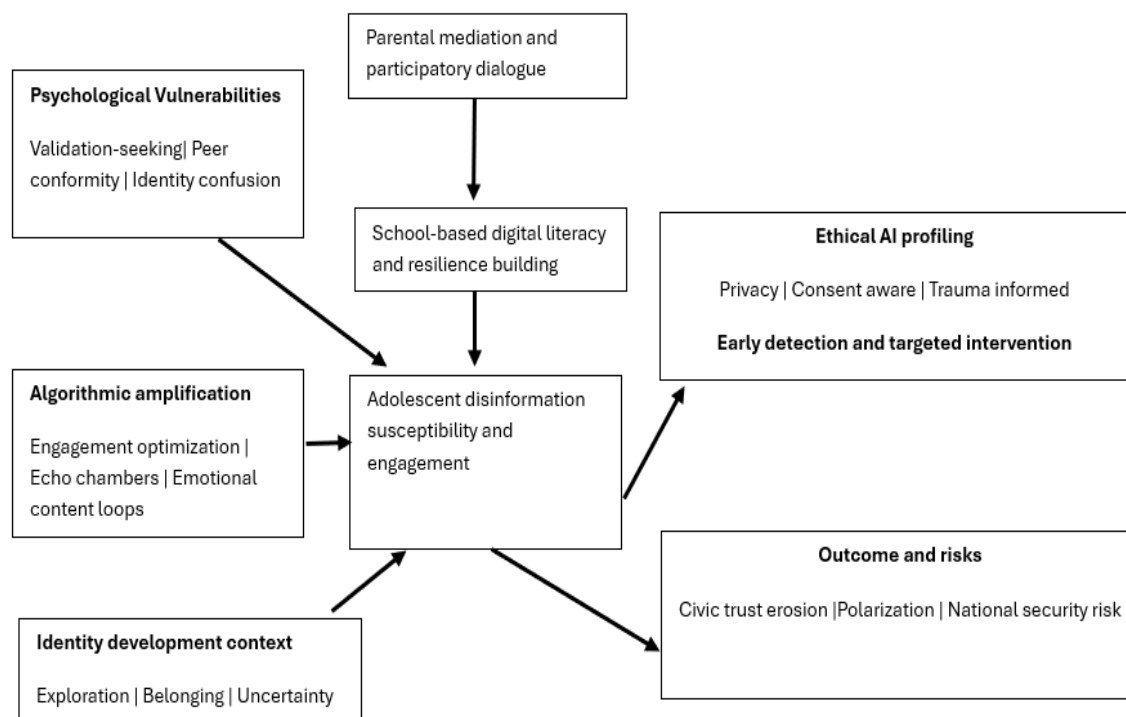


Figure no. 2: *Conceptual Framework of Drivers, Moderators, and Outcomes of Disinformation*
(Source: Created by authors)

Figure no. 2 illustrates the conceptual framework emerging from this review, highlighting how psychological vulnerabilities, algorithmic amplification, and identity development processes converge to increase adolescent susceptibility to disinformation. These drivers interact dynamically, shaping both engagement with and reinforcement of harmful content. The framework also emphasizes the protective role of parental mediation and school-based digital literacy programs, which serve as buffers that can strengthen resilience. Ethical AI profiling is presented as a potential intervention pathway, offering opportunities for early detection and targeted support when designed with transparency, consent, and developmental sensitivity. The model underscores that adolescent disinformation engagement is not solely a matter of individual behavior but rather a systemic interaction of cognitive, social, and technological forces with profound implications for civic trust and national security.

8. Limitations

This conceptual perspective paper, while integrative, has several limitations. A key constraint is its reliance on a synthesis of insights from psychology, cybersecurity, and AI ethics literature, rather than primary data, which limits generalizability. The diversity within adolescent populations across socioeconomic, neurocognitive, and cultural lines is vast and not fully explored here. Moreover, the complex geopolitical landscape of AI governance and platform regulation introduces variability that a single-nation framework cannot fully capture. Lastly, although the paper emphasizes the need for ethical AI design, a more in-depth examination of technical implementation is required, underscoring the importance of interdisciplinary collaboration between social scientists and engineers.

9. Policy Recommendations

To mitigate adolescent exposure to disinformation and unethical AI profiling,

this paper recommends a multi-tiered policy approach, comprising the following actions:

- Enact algorithmic accountability legislation, that requires platforms to disclose their recommendation systems and profiling mechanisms, with independent auditing bodies assessing compliance and potential harm.

- Develop adolescent-centric digital rights frameworks, building on the principles of the UNCRC, to regulate data collection, use, and profiling. Policymakers should craft age-appropriate data protection policies that define how adolescent data can be collected, used, and profiled. This includes regulations on behavioral advertising, psychographic targeting, and AI-based risk prediction.

- Establish platform governance and cognitive security mandates. National security agencies and technology regulators should develop “cognitive threat intelligence” capabilities to detect and dismantle disinformation campaigns targeting youth populations. This should be embedded into national cybersecurity strategies as a preventive measure.

- Create cross-sectoral task forces to develop ethical design standards for adolescent-facing technology and content moderation practices. Dedicated task forces comprising educators, forensic psychologists, AI ethicists, child protection services, and platform designers should be established to develop ethical design standards for adolescent-facing technology and content moderation practices that align with developmental sensitivity.

- Prioritize funding for digital resilience programs in schools, particularly in underserved areas, to build psychological immunity against manipulation and extremist narratives. Public investment should prioritize digital resilience programs in schools, particularly in underserved areas, to build psychological immunity against ideological manipulation, misinformation, and extremist recruitment narratives. These policy recommendations aim to provide a

comprehensive framework for protecting adolescents from the risks associated with disinformation and unethical AI profiling. These recommendations aim to provide a comprehensive framework for protecting adolescents from the risks associated with disinformation and unethical AI profiling.

10. Conclusions

This paper highlights the adolescent demographic as a critical vulnerability point in the evolving threat landscape of disinformation and algorithmic profiling. By applying a forensic cyberpsychology lens, we have demonstrated how the intersection of adolescent cognitive, emotional, and social vulnerabilities with AI-driven profiling systems creates an environment conducive to manipulation. This is not a coincidental byproduct of the digital age, but rather a vulnerability strategically exploited by hostile actors seeking to undermine societal cohesion and national stability through psychological and ideological infiltration (Ohu & Jones, 2025d). The analysis reveals that adolescent engagement with digital content extends beyond individual media choices, representing a systemic vulnerability in national cognitive infrastructure. Therefore, protecting adolescents is not only a developmental or educational concern, but a national security imperative. The convergence of AI, big data profiling, and persuasive design necessitates urgent attention to the ethical governance of digital platforms, particularly those popular among youth (Huang et al., 2024; Chng et al., 2025). This study presents a high-level synthesis of psychological, technological, and geopolitical factors, along with a call to action, to reimagine adolescent digital safety through multidisciplinary collaboration. By adopting a forensic cyberpsychology approach, we can gain diagnostic clarity and develop effective intervention pathways that integrate ethical AI practices, educational innovation, and robust policy mechanisms.

10.1. Practical Implications

The findings of this paper highlight an urgent need for reforms in how technology platforms, educators, and policymakers address adolescent interactions with AI-curated environments. From a forensic cyberpsychology perspective, this urgency stems from the convergence of psychological vulnerabilities such as validation-seeking and identity confusion with algorithmic systems that amplify harmful content (Ohu & Jones, 2025d). For instance, evidence from adolescent disinformation studies shows that emotionally charged content is disproportionately recommended, creating a cycle of psychological reinforcement that mirrors forensic markers of manipulation. By embedding algorithmic transparency and mandating independent audits, stakeholders can begin to break this cycle (Solyst et al., 2025). Analysis of these reforms demonstrates how early-warning systems, such as ethical AI profiling designed with developmental sensitivity, can serve as preventive forensic tools to detect patterns of susceptibility without infringing on autonomy. This links directly to the evolution of forensic cyberpsychology practice by demonstrating that digital risk detection is not only about identifying offenders but also about protecting vulnerable populations before harm occurs.

The broader practical implications extend beyond education into governance and duty of care. Governments and private technology companies must adopt governance protocols that ensure adolescent data are handled under age-appropriate standards. Evidence from national security frameworks underscores that disinformation exposure among youth erodes civic trust and can destabilize democratic processes (Ahmed et al., 2025). When forensic cyberpsychology approaches are applied here, they reveal that adolescent digital vulnerability is not incidental but a systemic risk demanding structured oversight. Analysis shows that operationalizing ethical principles into

platform design and regulation transforms forensic cyberpsychology practice from reactive investigations into proactive prevention. Linking back to innovation in forensics, this paradigm shift redefines the field as one equally concerned with safeguarding psychological well-being and protecting national cognitive infrastructure.

10.2. Social Implications

The risks outlined in this paper emphasize that adolescent susceptibility to disinformation is not confined to individual development but reverberates through families, communities, and national systems. Forensic cyberpsychology approaches illustrate how adolescents serve as both consumers and amplifiers of disinformation, meaning their vulnerabilities can polarize communities and erode social cohesion. Evidence from studies on digital echo chambers confirms that peer conformity and social identity pressures amplify susceptibility, leading to intergenerational divides. Analysis of these findings demonstrates that without ethical oversight, society risks producing a generation predisposed to cynicism and distrust (Romanishyn et al., 2025; Shin et al., 2022; Warin, 2024). By situating this within forensic cyberpsychology discourse, the role of social systems becomes clearer, disinformation is not only a national security issue but also a forensic cyberpsychology concern tied to collective psychological health and social resilience.

The social duty of care extends into designing digital ecosystems that foster resilience rather than division. Evidence from participatory governance models shows that including adolescents in shaping digital policy increases their sense of agency and mitigates susceptibility to manipulative ideologies (Ohu & Jones, 2025b). Forensic cyberpsychology reframes this involvement as both a protective measure and a diagnostic tool for identifying societal vulnerabilities. Analysis demonstrates that when parents, educators, and policymakers'

model responsible digital behaviors, they embody forensic cyberpsychology principles of ethical oversight and duty of care. Linking this back to innovation in forensic approaches, the shift is evident. Forensic inquiry now encompasses not only the investigation of wrongdoing but also the proactive cultivation of environments where manipulative behaviors are less likely to take root, strengthening the social fabric necessary for democratic resilience (Ohu & Jones, 2025a).

10.3. Practice Implications

From a professional practice standpoint, this paper underscores the need for ethical and developmental sensitivity in designing interventions. Forensic cyberpsychology provides a framework for practitioners to detect early behavioral markers of susceptibility, such as impulsive content sharing or digital validation-seeking. Evidence from trauma-informed intervention models demonstrates that targeted counseling can reduce adolescents' likelihood of engagement with manipulative content. Analysis shows that forensic cyberpsychology extends traditional forensic practices by equipping educators, psychologists, and policymakers with a preventive lens, one that identifies and disrupts digital manipulation before it escalates (Ohu & Jones, 2025d). Linking this to innovation in forensic cyberpsychology, the emphasis shifts from post-incident investigation to pre-emptive, developmental, and systemic risk management.

Governance and oversight practices further reflect these forensic implications. Evidence from algorithmic accountability studies shows that binding standards and auditing mechanisms can reduce the risks of exploitative profiling (Ganapathy, 2024). By adopting forensic cyberpsychology approaches, policymakers and engineers can design systems that are explainable, age-sensitive, and ethically aligned. Analysis reveals that this integration transforms duty of care from a reactive legal safeguard into a proactive mandate, one that protects

adolescents as both individuals and members of a vulnerable population. Linking back to innovative forensic cyberpsychology thinking, this demonstrates how codes of conduct in psychology, education, and technology must evolve to encompass algorithmic ethics, thereby expanding the scope of forensic inquiry into the digital ecosystem.

10.4. Theoretical Implications

The theoretical frameworks in this paper illuminate how forensic cyberpsychology can redefine our understanding of adolescent disinformation risks. Evidence from Erikson's psychosocial theory and Dual-Process Cognition shows that adolescence is a stage where identity confusion and impulsive emotional reasoning intersect with algorithmic amplification. Analysis of these frameworks through a forensic lens highlights the urgency of developing ethical oversight systems, as adolescent vulnerabilities create predictable patterns of susceptibility that can be exploited by hostile actors. This integration underscores that disinformation is not a random byproduct of technology but a foreseeable outcome when developmental immaturity meets unregulated governance (Ohu & Jones, 2025b; Shin et al., 2022). Linking back to innovation in forensics, this reflects a shift toward conceptualizing cognitive manipulation itself as a forensic cyberpsychology risk category.

The ethical and governance dimensions of these theories become more pronounced when framed through forensic cyberpsychology. Evidence from Social Identity Theory and Cognitive Behavioral Theory shows that peer conformity and maladaptive thinking patterns heighten risk but also provide intervention pathways for resilience (Pérez-Torres, 2024; Sørensen et al., 2025). Analysis demonstrates that oversight mechanisms rooted in these theories can guide the creation of AI systems that are transparent, developmentally appropriate, and ethically sound. Linking to forensic innovation, this theoretical reframing represents a paradigm

shift: forensic science is no longer confined to crime scene analysis or offender profiling but extends into safeguarding adolescents from algorithmic manipulation. This expansion of scope redefines the duty of care as a forensic obligation, embedding ethics and governance into the core of digital-era forensic cyberpsychology practice.

10.5. Recommendations for Future Research

– Modified Delphi Technique

Future research should consider employing the Modified Delphi Technique as a structured approach to achieving consensus among experts across disciplines such as forensic psychology, adolescent development, AI ethics, and national security (Arribas et al., 2025; Niederberger & Deckert, 2022; Niederberger & Köberich, 2021). The advantage of this method lies in its iterative design, which allows participants to refine and reassess their views anonymously over multiple rounds, reducing the influence of hierarchy and groupthink. In the context of forensic cyberpsychology, the Delphi Technique is particularly beneficial for synthesizing expert judgments about ethical AI profiling, adolescent vulnerabilities, and intervention strategies where empirical evidence is still emerging. Its utility lies in generating actionable consensus that can guide the development of early-warning systems and policy recommendations, ensuring that diverse professional insights converge to address the complexities of adolescent disinformation and algorithmic amplification.

– Action Research

Another promising avenue for future inquiry is the application of Action Research, which emphasizes iterative cycles of planning, acting, observing, and reflecting in real-world contexts (Casey et al., 2025). This method offers the advantage of situating research within the environments where adolescents engage with digital platforms, thereby producing findings that are both contextually grounded and practically

relevant. For forensic cyberpsychology, Action Research allows collaboration between researchers, educators, platform designers, and adolescents themselves to co-create interventions that build digital resilience and ethical technology use. The benefit of this method lies in its participatory nature, which empowers adolescents as stakeholders rather than passive subjects, aligning with the broader duty of care discussed in this paper. Its utility is clear. Action Research provides a framework for testing and refining digital literacy curricula, parental mediation models, and AI monitoring tools in situ, ensuring interventions are adaptable, developmentally sensitive, and ethically sound.

– **Implementation Science**

Finally, Implementation Science offers a valuable framework for examining how forensic cyberpsychology-informed interventions can be effectively integrated into schools, communities, and national security infrastructures. Implementation Science distinguishes itself through its systematic focus on the conditions that enable or hinder real-world adoption of evidence-based interventions. A scoping review by Fontaine et al. (2025) develops the SELECT-IT meta-framework, which

structures *Theories, Models, and Frameworks* (TMF) selection across four evaluative steps, considering both theoretical strengths, such as clarity, equity, scientific robustness, and real-world constraints, which include team readiness, resource availability, and project fit. This method ensures that program designs extend beyond conceptual promises, aligning with situational realities to produce measurable impact. The advantage of this method lies in its systematic focus on identifying barriers and facilitators to real-world adoption, ensuring that programs move beyond theoretical design to measurable impact. In the field of adolescent disinformation, Implementation Science provides tools to evaluate the scalability of AI-driven risk detection systems, the sustainability of media literacy programs, and the long-term effectiveness of policy mandates. The benefit is its emphasis on bridging the gap between research and practice, ensuring that interventions are not only evidence-based but also contextually feasible (Fontaine et al., 2025). Its utility for forensic applications lies in its capacity to align ethical AI design with institutional governance, thereby embedding the duty of care into everyday practice across educational, technological, and policy domains.

REFERENCES

- Ahmed, S., Masood, M., Bee, A.W.T., & Ichikawa, K. (2025). False failures, real distrust: the impact of an infrastructure failure deepfake on government trust. *Frontiers in Psychology*, Vol. 16. Available at: <https://doi.org/10.3389/fpsyg.2025.1574840>.
- Amsari, D., Wahyuni, E., & Fadhilaturrahmi, F. (2024). The Social Learning Theory Albert Bandura for Elementary School Students. *Jurnal Basicedu*, 8(2), 1654-1662. Available at: <https://doi.org/10.31004/BASICEDU.V8I2.7247>.
- Arribas, C.M., Arcos, R., & Gertrudix, M. (2025). Application of the Delphi methodology to forecast competencies oriented towards AI-driven disinformation detection in an expanded DigComp framework. *MethodsX*, Vol. 14. Available at: <https://doi.org/10.1016/J.MEX.2025.103401>.
- Brassil, M., O'Mahony, C., & Greene, C.M. (2024). Do cognitive abilities reduce eyewitness susceptibility to the misinformation effect? A systematic review. *Psychonomic Bulletin and Review*, 31(6), 2410-2436. Available at: <https://doi.org/10.3758/S13423-024-02512-5>.

Braun, V., & Clarke, V. (2024). Supporting best practice in reflexive thematic analysis reporting in *Palliative Medicine: A review of published research and introduction to the Reflexive Thematic Analysis Reporting Guidelines (RTARG)*. *Palliative Medicine*, 38(6), 608-616. Available at: <https://doi.org/10.1177/02692163241234800>.

Burrell, D.N. (2024). Exploring the Cyberpsychology of Social Media Addiction and Public Health Risks among Black American Women in the USA. *Health Economics and Management Review*, 5(2), 14-31. Available at: <https://doi.org/10.61093/hem.2024.2-02>.

Byrne, A., Martin, D., Jones, C., Galbraith, N., & Mercer, T. (2024). Conspiracy theory beliefs in the adolescent population: A systematic review. *Journal of Adolescence*, 96(5), 925-939. Available at: <https://doi.org/10.1002/JAD.12316>.

Casey, M., Coghlan, D., Carroll, Á., & Stokes, D. (2025). A tool for theory development in action research: a challenge and a resource for nursing research. *International Journal of Nursing Studies Advances*, 8, 100357. Available at: <https://doi.org/10.1016/J.IJNSA.2025.100357>.

Chng, S.Y., et al. (2025). Ethical considerations in AI for child health and recommendations for child-centered medical AI. *NPJ Digital Medicine*, 8(1), 152. Available at: <https://doi.org/10.1038/s41746-025-01541-1>.

Crone, E.A., & van Drunen, L. (2024). Development of Self-Concept in Childhood and Adolescence: How Neuroscience Can Inform Theory and Vice Versa. *Human Development*, 68(5-6), 255-271. Available at: <https://doi.org/10.1159/000539844>.

Fontaine, G., et al. (2025). Advancing the selection of implementation science theories, models, and frameworks: a scoping review and the development of the SELECT-IT meta-framework. *Implementation Science*, 20(1), 1-24. Available at: <https://doi.org/10.1186/S13012-025-01436-5/PEER-REVIEW>.

Ganapathy, V. (2024). AI-Based Risk Assessments in Forensic Auditing: Benefits, Challenges and Future Implications. *Shodh Sari-An International Multidisciplinary Journal*, 03(04), 100-128. DOI: <https://doi.org/10.59231/SARI7750>.

Huang, S., et al. (2024). AI Technology panic – is AI Dependence Bad for Mental Health? A Cross-Lagged Panel Model and the Mediating Roles of Motivations for AI Use Among Adolescents. *Psychology Research and Behavior Management*, 17, 1087. Available at: <https://doi.org/10.2147/PRBM.S440889>.

Lemaire, M., Ye, S., Le Stanc, L., Borst, G., & Cassotti, M. (2025). The development of media truth discernment and fake news detection is related to the development of reasoning during adolescence. *Scientific Reports*, 15(1), 1-10. Available at: <https://doi.org/10.1038/S41598-025-90427>.

Li, Q., Tang, W., & Liu, X. (2025). Value-Directed Remembering: A Dual-Process Perspective. *Behavioral Sciences*, 15(8), 1113. Available at: <https://doi.org/10.3390/BS15081113>.

Murad, H.R.J. (2024). Investigating The Impact of Digital Technology on Adolescent Identity Formation on Selected Students in SAIS: A Psychological Approach. *International Journal of Innovative Science and Research Technology (IJISRT)*, 2726-2736. Available at: <https://doi.org/10.38124/IJISRT/IJISRT24APR1823>.

Niederberger, M., & Deckert, S. (2022). The Delphi technique: Methodology, variants and usage examples[Formula presented]. *Zeitschrift Fur Evidenz, Fortbildung Und Qualitat Im Gesundheitswesen*, 174, 11-19. Available at: <https://doi.org/10.1016/j.zefq.2022.08.007>.

Niederberger, M., & Köberich, S. (2021). Coming to consensus: The Delphi technique. *European Journal of Cardiovascular Nursing*, 20(7), 692-695. Available at: <https://doi.org/10.1093/EURJCN/ZVAB059>.

Ohu, F.C., & Jones, L.A. (2025a). An examination of digital validation-seeking behaviors in adolescents as precursors to romance scamming. *Scientia Moralitas Conference Proceedings*, 10-29. DOI:10.5281/zenodo.14911844.

Ohu, F.C., & Jones, L.A. (2025b). AI-driven forensic cyberpsychology intervention strategies for social media platform and school managers to mitigate cyber fraud at-risk adolescents. *Scientia Moralitas Conference Proceedings*, 114-131. Available at: DOI:10.5281/zenodo.15075890.

Ohu, F.C., & Jones, L.A. (2025c). Validation syndrome: The root of deception and developmental predictors of dark triad traits in adolescents for forensic and developmental psychology. *International Educational Research*, 8(2), 67-86. Available at: <https://doi.org/10.30560/ier.v8n2p67>.

Ohu, F.C., & Jones, L.A. (2025d). The Intersection of Cyberwarfare, Social Media, and Adolescent Self- Esteem: A Forensic Cyberpsychology Analysis. *International Conference on Cyber Warfare and Security*, 20(1), 332-344. Available at: <https://doi.org/10.34190/ICCWS.20.1.3375>.

Owens, E. (2024). Teens on TikTok: Understanding Young People's Digital Agency as Practice. *International Research in Children's Literature*, 17(2), 174-188. Available at: <https://doi.org/10.3366/IRCL.2024.0562>.

Park, J., Akter, M., Ali, N.S., Agha, Z., Alsoubai, A., & Wisniewski, P. (2025). Towards Resilience and Autonomy-based Approaches for Adolescents Online Safety. *SSRN Electronic Journal*. Available at: <https://doi.org/10.2139/ssrn.4608406>.

Pérez-Torres, V. (2024). Social media: a digital social mirror for identity development during adolescence. *Current Psychology*, 43(26), 22170-22180. Available at: <https://doi.org/10.1007/s12144-024-05980-z>.

Rai, S. (2025). Reimagining Learning: The Relevance and Application of Constructivist Theory in 21st Century Classrooms. *IJFMR - International Journal For Multidisciplinary Research*, 7(4). Available at: <https://doi.org/10.36948/IJFMR.2025.V07I04.50004>.

Raufelder, D., Hoferichter, F., Kulakow, S., Golde, S., Gleich, T., Romund, L., Lorenz, R.C., Pelz, P., & Beck, A. (2021). Adolescents' Personality Development – A Question of Psychosocial Stress. *Frontiers in Psychology*, 12, 785610. Available at: <https://doi.org/10.3389/FPSYG.2021.785610/BIBTEX>.

Romanishyn, A., Malytska, O., & Goncharuk, V. (2025). AI-driven disinformation: policy recommendations for democratic resilience. *Frontiers in Artificial Intelligence*, 8, 1569115. Available at: <https://doi.org/10.3389/FRAI.2025.1569115/BIBTEX>.

Saha, M., Pagadala, P.K., & Basu, M.T. (2024). Cyber Deceptions: Unveiling the Threat of Deepfakes in Digital Realms. *ICCCMLA 2024 – 6th International Conference on Cybernetics, Cognition and Machine Learning Applications*, 113-116. Available at: <https://doi.org/10.1109/ICCCMLA63077.2024.10871909>.

Shin, D., et al. (2022). Countering Algorithmic Bias and Disinformation and Effectively Harnessing the Power of AI in Media. *Journalism & Mass Communication Quarterly*, 99(4), 887-907. Available at: <https://doi.org/10.1177/10776990221129245>.

Shin, D., & Jitkajornwanich, K. (2024). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review*, 42(4), 1020-1040. Available at: <https://doi.org/10.1177/08944393231225547>.

Solyst, J., et al. (2025). Investigating Youth AI Auditing. *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2098-2111. Available at: <https://doi.org/10.1145/3715275.3732142>.

Sørensen, N.M., Skaarnes, H., Mathiasen, K., Thastum, M., & Lomholt, J.J. (2025). Developing an Internet-Based Cognitive Behavioral Therapy Intervention for Adolescents with Anxiety Disorders: Design, Usability, and Initial Evaluation of the CoolMinds Intervention. *JMIR Formative Research*, 9(1), e66966. Available at: <https://doi.org/10.2196/66966>.

Szabó, Z.P., Orosz, N.Z., Gulyás, R., & Láng, A. (2024). The Associations of Peer-Rated Popularity and Likeability with Dark Triad Personality Traits in Adolescent Groups. *Europe's Journal of Psychology*, 20(3), 165-177. Available at: <https://doi.org/10.5964/EJOP.11667>.

Warin, T. (2024). *Disinformation in the Digital Age: Impacts on Democracy and Strategies for Mitigation*. Available at: <https://doi.org/10.2139/SSRN.4995571>.

Zucchelli, M.M., Matteucci Armandi Avogli Trotti, N., Pavan, A., Piccardi, L., & Nori, R. (2025). The Dual Process model: the effect of cognitive load on the ascription of intentionality. *Frontiers in Psychology*, 16, 1451590. Available at: <https://doi.org/10.3389/FPSYG.2025.1451590/BIBTEX>.