Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

CYBER-VICTIMOLOGY IN PRACTICE: CONCEPTUALIZING CYBERBULLYING AND DESIGNING PREVENTION SYSTEMS

Nozimakhon Sobirova
Teacher, Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Uzbekistan

Abstract

Cyberbullying has become a salient form of adolescent victimization, shaped by the affordances of social networks and the routine integration of digital communication into youth daily life. This article develops a comparative criminological synthesis of cyberbullying as a distinct yet overlapping phenomenon with offline bullying, using a structured review approach and drawing on empirical indicators highlighted in recent international and national sources (2018–2024). The analysis foregrounds three interconnected domains: (1) prevalence and trends, including evidence that cyberbullying has reached parity with, and in some contexts surpasses, traditional bullying; (2) risk architecture, emphasizing intensity of social media exposure, digital competence and online practices, and socio-demographic vulnerability; and (3) mechanisms of harm specific to digital environments—anonymity, scalability of audiences, persistence of harmful content, and the 24/7 reach that increases revictimization. A focused national lens is provided through Uzbekistan, where PISA-2022-based indicators suggest that approximately one in six 15-year-old students experiences recurring bullying, with measurable academic losses and elevated vulnerability among boys, migrants, and urban students. The article concludes that effective prevention requires a multi-level strategy integrating schools, families, platforms, and state policy, and argues for the development of "cyber-victimology" as a criminological sub-field to strengthen early detection, evidence-based intervention, and holistic rehabilitation.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

Keywords: Cyberbullying; adolescent victimization; social media; digital literacy; criminology; prevention

1. INTRODUCTION

Over the past decade, social networks have reconfigured adolescent interaction, expanding opportunities for communication while simultaneously creating new vectors of aggression. Cyberbullying—intentional and repeated harassment using digital technologies—includes abusive messages, humiliating images and videos, rumor dissemination, doxxing-like publication of personal data, and the use of fake accounts for ridicule. Unlike many offline episodes, cyberbullying can occur without co-presence, can be amplified to unlimited audiences, and can persist through reposts, screenshots, and algorithmic resurfacing of harmful content. These properties intensify victimization and complicate prevention, attribution, and remediation.

The public-health and criminological relevance of cyberbullying is increasingly recognized, given associations with anxiety, depression, suicidal ideation, and other adverse outcomes. In comparative perspective, reported cyberbullying prevalence in industrialized contexts commonly ranges from single digits to around one fifth of adolescents, and evidence indicates gradual increases in digital harassment alongside stable or declining levels of some offline bullying where prevention programs are implemented.

This article advances a criminological synthesis with two objectives. First, it clarifies cyberbullying as a form of victimization with distinctive situational and social mechanisms while remaining entangled with offline bullying dynamics. Second, it integrates a national evidence lens for Uzbekistan, where recent policy developments and PISA-based indicators create an opportunity to connect victimization measurement with education outcomes and prevention design.

2. METHODS (REVIEW DESIGN AND ANALYTIC FRAME)

Design. The study follows a structured comparative-analytic review logic aligned with an IMRAD-style organization, synthesizing published international and national materials and extracting comparable indicators across four analytic

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

blocks: (1) prevalence and trends; (2) risk factors; (3) mechanisms and situational dynamics; and (4) prevention and countermeasures.

Data base. The evidence base, as reflected in the underlying text, includes international reviews and surveys, cross-national analyses of social media use and cyberbullying, and policy-relevant sources (e.g., large-scale education survey indicators and national legal developments). Key reference anchors include PISA-2022 bullying-related indicators and cross-national findings on cyberbullying prevalence and risk factors.

Limitations. The synthesis inherits typical limitations of secondary-data reviews: definitional inconsistency across studies (what counts as "cyberbullying"), differences in recall periods and measurement instruments, and uneven national data availability. For Uzbekistan specifically, the review relies on available survey-based indicators and policy references rather than a dedicated national cyberbullying prevalence measurement system.

3. RESULTS

3.1. Prevalence and trends: online vs offline victimization

The extant data indicate that the prevalence of cyberbullying among adolescents has approached that of offline bullying in a number of contexts, and may exceed it in some countries. A salient trend that has emerged is the prevalence of cyberbullying among adolescents. According to regional surveys, approximately one in six adolescents have reported experiencing cyberbullying, marking an increase from previous survey waves. Concurrently, offline bullying continues to affect approximately one in ten adolescents, as indicated by aggregate estimates.

Cyberbullying and traditional bullying often co-occur: offline aggressors may extend harassment into digital spaces, and offline victims may experience continued abuse online. This overlap matters for criminological interpretation because it suggests shared offender networks and situational continuity rather than two isolated phenomena.

In the PISA-2022 study, which assessed bullying among 15-year-olds in Uzbekistan, 17.1% of 7,293 students in 202 schools reported having experienced some form of bullying at least several times a month. The most prevalent forms

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

of bullying were as follows: verbal abuse (21%), the dissemination of rumors (16%), physical aggression resulting in injuries on school grounds (16%), and damage or theft of personal belongings (14%). Of particular note is the prevalence of extortion, which has been a recurring theme in the annals of history. A survey revealed that 4.2% of respondents reported having paid money to bullies at least once during the previous year. This figure is almost double the OECD average cited in the same discussion.Risk stratification in Uzbekistan. The same evidence summary identifies higher victimization among boys (19.1% vs. 15.4% for girls), among students with migrant status or children of migrants (30.6% vs. 17.1% for non-migrants), and among urban students (19.4% vs. 15.6% rural). These disparities are important for targeted prevention, as they imply structural and contextual vulnerability beyond individual behaviors.

The text further reports an econometric interpretation (REPEST-based) connecting perceived school safety and bullying exposure to PISA performance. A one standard deviation decrease in the subjective school safety index is associated with lower PISA scores (about −5.2 in mathematics, −6.2 in reading, −4.7 in science). Regular bullying exposure is associated with an additional reduction of about 18–20 points across domains; extortion is described as the most damaging (−57.6 mathematics; −67.4 reading; −67.0 science), framed as roughly 1.5–2 academic years of lost progress for extortion victims.

3.2. Risk architecture: exposure, competence, and socio-demographics

The amount of time spent engaging with online content, particularly on social networking platforms, has been identified as a significant predictor of risk. Research has demonstrated a positive correlation between increased exposure to online content and the likelihood of victimization. This pattern aligns closely with the perspectives of lifestyle exposure and routine activity. It suggests that adolescents who maintain a substantial digital "routine presence" become more susceptible to targeting, while effective guardianship—whether provided by parents, schools, or platform intermediaries—may be intermittent or structurally constrained.

Concurrently, the risk appears to be contingent not solely on the magnitude of online activity but also on the manner in which adolescents engage with the

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

internet. A particular emphasis is placed on behaviors that increase vulnerability, such as extensive self-disclosure, the addition of unfamiliar contacts, and engagement in antagonistic exchanges. The analysis also indicates a paucity of awareness regarding privacy settings and practical coping strategies. Within this logic, digital literacy functions as a protective resource. Conversely, insufficient competence can heighten susceptibility by undermining timely documentation of incidents and reducing the likelihood of effective reporting.

The synthesis further indicates that exposure and harm are distributed unevenly across demographic and social vulnerability dimensions. A preliminary investigation of aggregated statistics reveals the possibility of slightly higher rates of cybervictimization among girls. However, further analysis is necessary to determine whether boys are more frequently represented among perpetrators. The text also emphasizes heightened targeting tied to visible or perceived difference—such as appearance, race/ethnicity, and gender or sexual identity—patterns that align with status-based victim selection and group-oriented hostility.

Finally, psychosocial and family-context factors are treated as important correlates of victimization and potential drivers of revictimization cycles. Depression, anxiety, and low self-esteem are highlighted as risk-linked conditions, particularly where combined with adverse or conflictual family environments. Conversely, supportive family relationships and open, trust-based communication are presented as protective, strengthening adolescents' capacity to seek help, activate safeguards, and recover from harmful digital encounters.

3.3. Mechanisms specific to cyberspace

The phenomenon of anonymity and the absence of social constraints have been identified as contributing factors. A fundamental aspect of cyberbullying is the use of anonymity by the offenders, which can lead to a reduction in social inhibitions and the facilitation of cruelty in the absence of immediate interpersonal feedback. This condition also heightens victims' uncertainty about who is responsible, a dynamic that can broaden fear and suspicion beyond the original incident. Consequently, the harm may intensify not only due to the

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

challenge of directly confronting aggression, but also because informal resolution becomes more arduous when identity is ambiguous.

The concepts of persistence, scalability, and revictimization are of particular concern. The phenomenon of cyberbullying is not constrained by temporal or geographical boundaries, capable of unfolding in an uninterrupted manner, thereby progressively eroding the "safe spaces" that may be present in offline environments. The dissemination of harmful material through shares, reposts, and other forms of online interaction can persist, persisting long after the initial incident, thereby creating cycles of revictimization. The potential for a vast audience further amplifies the consequences of reputational damage and emotional distress, particularly for adolescents whose sense of self and social standing is profoundly influenced by peer perception.

The role structure of the incident included the aggressor, the victim, and bystanders. Digital platforms have expanded the concept of bystander participation, transforming it into a diffuse and frequently substantial audience capable of amplifying harm through seemingly trivial actions such as liking, commenting, forwarding, or reposting content. In such circumstances, the concept of responsibility may become obscured, thereby reducing the probability of peer intervention. Concurrently, effective utilization of platform reporting mechanisms has the potential to translate guardianship into scalable action by facilitating the implementation of expeditious flagging, moderation, and removal procedures.

3.4. Prevention and countermeasures: a multi-level model

Digital literacy education is presented as a foundational pillar of prevention. This encompasses not only technical competencies but also privacy management, secure communication practices, preservation of digital evidence, understanding of reporting and complaint procedures, and the cultivation of empathy and responsible online norms. It is imperative to acknowledge that the efficacy of such training is maximized when it is integrated into institutional routines and curricula, as opposed to its delivery as isolated, short-term campaigns.

At the family level, the emphasis is placed on a balanced model of supervision. Trust-based communication and supportive monitoring are preferable to

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

punitive control, which may unintentionally encourage concealment and delay help-seeking. Practical measures to be implemented include explicit family agreements on online conduct, reasonable boundaries for time and content, and improvements in parents' own digital competence so that guidance is credible and actionable.

Schools have been established as the primary institutional nexus for intervention, even in cases where specific incidents occur off-campus. Given that adolescent peer networks typically encompass both school life and social media spaces, effective responses necessitate clear school policies and operational procedures. The intervention repertoire highlighted in the text includes "zero tolerance" approaches, confidential reporting channels, access to psychological support, and the use of evidence-based prevention programs that combine universal measures with case-based responses.

In Uzbekistan, the preventive architecture is further supported by a legal and governance framework. The country has adopted a framework law on protecting children from all forms of violence (ZRU-996, November 14, 2024), which defines bullying as a form of harassment and explicitly obliges educational institutions to prevent, document, and investigate bullying incidents, as well as to cooperate with relevant services. This legal foundation strengthens standard-setting, incident registration, and inter-agency coordination.

The text also underscores the role of evidence-based program adoption. With the support of UNICEF, Uzbekistan has developed a plan to implement the Finnish KiVa program and the Italian No Trap! program in 30 schools across Tashkent, Bukhara, and Fergana. The design integrates primary prevention, facilitated by curriculum modules and parent engagement, with targeted intervention strategies. These intervention strategies include structured support for victims and behavioral correction components for aggressors.

In conclusion, platform governance is regarded as an integral component of "distributed guardianship." Platforms contribute to this effort through the implementation of moderation instruments, the establishment of reporting pathways, the automation of the detection of abusive language, and the incorporation of design features that can mitigate impulsive harm (e.g., the implementation of warning prompts prior to posting). Concurrently, the text

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

acknowledges structural constraints, encompassing evasion through novel or alternative accounts, and the suboptimal accuracy and consistency of moderation practices.

4. DISCUSSION

4.1. Interpreting cyberbullying through criminological theory

A key contribution of the synthesis is conceptual: cyberbullying is not merely "bullying moved online," but a victimization configuration shaped by the criminogenic properties of digital environments. The affordances of anonymity, persistence, and scalability change the cost–benefit profile for offenders and amplify harm for victims. These properties also transform guardianship: whereas offline guardianship is spatially localized (teachers, supervisors), online guardianship is distributed across parents, peers, platform moderators, and automated systems—often with gaps.

The extant evidence base of the study supports an exposure-oriented risk model. Specifically, the study found that increased active use of social media and risky practices increases the likelihood of victimization, while digital literacy and support from others reduce it. This finding aligns with the tenets of routine activity theory, which posits the presence of targets for offenders and a weakening of supervision. It is also consistent with lifestyle impact reasoning, which conceptualizes the digital lifestyle as a structured environment.

4.2. Uzbekistan: from measurement to policy design

Uzbekistan's PISA-linked bullying indicators matter not only as prevalence measures but also because the reported academic losses provide a policy-relevant bridge between child protection and education outcomes. The scale of losses associated with extortion is particularly salient, suggesting that anti-bullying policy should treat coercive victimization as an education and safety priority rather than a peripheral disciplinary matter.

The combination of a new legal framework (ZRU-996) and planned evidence-based school program pilots creates an implementation window. The decisive question becomes institutional capacity: incident registration quality, staff

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

training, inter-agency referral pathways (education–social services–law enforcement), and monitoring and evaluation of interventions.

4.3. Toward "cyber-victimology" as a sub-field

This study provides indirect support for the development of "cyber victimology" as a distinct field of criminological and applied research. The focus of this field is on the early detection, prevention, and comprehensive rehabilitation of victims in the digital environment. This phenomenon is not merely a terminological innovation; rather, it reflects structural changes in the architecture of victimization caused by social networks and digital communication. Cyberbullying differs from conventional bullying not only by "place" (online vs. offline) but by core mechanism: digital harm is characterized by persistence of content, scalability of audiences, ambiguity of offender identity, rapid replication, and the collapse of temporal boundaries through 24/7 access. These properties create qualitatively different victim experiences—namely, heightened uncertainty, repeated exposure (revictimization), and intensified reputational damage—requiring specialized analytic tools and institutional responses.

From a methodological standpoint, cyber-victimology is justified on three grounds. First, the digital environment alters causal pathways and complicates attribution: anonymity and impersonation can obscure the offender–victim relationship and undermine informal resolution, while the role of "bystanders" expands into a large and often algorithmically amplified audience that can reinforce victimization through engagement dynamics. Second, the evidentiary dimension is distinct: cyberbullying incidents leave digital traces (messages, images, metadata, screenshots, repost chains) that can be preserved, authenticated, and analyzed, but only if victims and institutions possess the procedural literacy to document them correctly and promptly. Third, platform governance becomes an integral part of guardianship: reporting tools, moderation policies, algorithmic detection of abusive content, and friction-based design measures can either mitigate or inadvertently intensify harm, making platforms de facto co-regulators rather than neutral communication channels.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

Conceptually, cyber-victimology can be framed around four analytic pillars. The first pillar is "digital exposure and routine activity," treating time online, social media intensity, and interaction patterns as structured exposure settings that shape the convergence of motivated offenders, suitable targets, and insufficient guardianship. The second pillar is "victim vulnerability and resilience," integrating individual-level factors (digital competence, privacy practices, coping skills), psychosocial correlates (anxiety, depressive symptoms, self-esteem), and contextual factors (family climate, peer group norms, school safety). The third pillar is "harm mechanics," focusing on how persistence, publicness, and replicability of content amplify psychological and social damage compared to episodic offline incidents. The fourth pillar is "institutional response ecology," mapping how schools, families, child protection services, law enforcement, and platforms interact—and where gaps emerge—in prevention, reporting, investigation, and recovery pathways.

Operationally, the sub-field would prioritize a set of applied instruments and protocols. One priority is validated screening and case-identification tools suitable for schools and youth services, including brief questionnaires that capture frequency, modality (messaging, image-based humiliation, group harassment), and severity indicators (threats, extortion-like coercion, dissemination of intimate content), alongside "red flag" markers for self-harm risk. A second priority is risk stratification: practical models that distinguish low-intensity conflicts from systematic victimization; identify high-risk groups (e.g., students with high social media exposure, migrant background, or those reporting unsafe school climates); and integrate school-level safety indices with victimization indicators for targeted interventions. A third priority concerns digital evidence protocols: step-by-step procedures for preserving content (screenshots with context, URLs, timestamps), documenting the sequence of events, preventing further dissemination, and ensuring confidentiality—particularly important where institutional responsibilities to record and investigate are legally framed.

Another core domain is trauma-informed and restorative support. Cyber-victimology would emphasize minimizing secondary victimization by institutions (e.g., disbelief, blaming, forced public disclosure), providing

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

psychological first aid, and organizing rehabilitation plans that combine mental health support, peer reintegration, and (where appropriate) restorative or behavioral correction measures for aggressors. Importantly, digital environments often produce a reputational harm component, so rehabilitation includes not only emotional recovery but also "digital recovery": removal requests, documentation for takedown procedures, privacy tightening, and identity restoration strategies. Within school settings, this aligns with evidence-based anti-bullying programs that incorporate both universal prevention and case-based intervention, and can be linked to broader child protection frameworks and pilot programs already referenced in the source material.

Finally, cyber-victimology must be evaluative and policy-facing. The practical test of this sub-field is whether interventions measurably reduce victimization and its downstream outcomes, including educational impacts. The Uzbekistan evidence lens in the source text illustrates why such evaluation matters: bullying exposure is associated with substantial learning losses, and coercive forms (e.g., extortion) show particularly severe effects. That linkage provides a strong rationale for embedding cyber-victimology tools into education-sector monitoring and prevention systems, with clear indicators (incident rates, reporting latency, resolution outcomes, student safety indices) and periodic assessment of program effectiveness across school, family, and platform layers

5. CONCLUSION

Cyberbullying is a contemporary form of adolescent victimization that both overlaps with and diverges from offline bullying. The reviewed evidence underscores four stable propositions: cyberbullying is widespread and in many contexts approaching parity with traditional bullying; risk is structured by exposure intensity, digital competence, and socio-demographic vulnerability; cyberspace-specific mechanisms (anonymity, persistence, unlimited audiences, and 24/7 reach) amplify harm and revictimization; and effective prevention requires an integrated, multi-level governance model. In Uzbekistan, PISA-based indicators suggest that recurring bullying affects roughly one in six 15-year-olds and is associated with measurable learning losses, with particularly severe impacts linked to extortion-type victimization. The policy path forward

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

is therefore not limited to punitive responses but should prioritize evidence-based school programs, family engagement, platform accountability mechanisms, and a robust incident monitoring and support infrastructure anchored in the new child-protection legal framework.

REFERENCES

1. Anderson, M. (2017, December 28). Key trends shaping technology in 2017. Pew Research Center.
2. Balaji, N., Pai, K. B. H., Kotari, M., & Venkatesh, B. (2020). Cyberbullying in online/e-learning platforms based on social networks. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(3), 1132–1136.
3. Craig, W., Walsh, S. D., Harel-Fisch, Y., Fotti, S., & Pickett, W. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. Journal of Adolescent Health, 66(6S), S100–S108. https://doi.org/10.1016/j.jadohealth.2020.03.006
4. Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. Current Opinion in Psychology, 45, 101314. https://doi.org/10.1016/j.copsyc.2022.101314
5. Hinduja, S., & Patchin, J. W. (2014). Cyberbullying: Identification, prevention, & response. Cyberbullying Research Center.
6. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2011). Cyberbullying: Bullying in the digital age (2nd ed.). Wiley-Blackwell.
7. OECD. (2023). PISA 2022 results (Volume I): The state of learning and equity in education. OECD Publishing. https://doi.org/10.1787/53f23881-en
8. Pew Research Center. (2022). Teens and cyberbullying 2022.
9. Ray, G., McDermott, C. D., & Nicho, M. (2024). Cyberbullying on social media: Definitions, prevalence, and impact challenges. Journal of Cybersecurity, 10(1).
10. School violence and bullying: Global status report. (2017). UNESCO.
11. Sourander, A., Klomek, A. B., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., et al. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. Archives of General Psychiatry, 67(7), 720–728.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

12. Varela, J. J., Sánchez-Soto, P. A., Chuecas, J., Benavente, M., González, C., Acuña-Wagner, E. A., & Olaya-Torres, A. (2021). Cyberbullying, bullying and antisocial behavior among Chilean adolescents. Revista Latinoamericana de Ciencias Sociales, Niñez y Juventud, 16(2), 148–171. https://doi.org/10.11600/1692715x.1622326072021
13. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. Frontiers in Public Health, 9, 634909.
14. Republic of Uzbekistan. (2024, November 14). Law "On protecting children from all forms of violence" (ZRU-996). National database of legislation (lex.uz).