



CYBER-FACILITATED SEXUAL EXPLOITATION: A SYSTEMATIC LITERATURE REVIEW OF RISK FACTORS, VICTIM VULNERABILITIES, OFFENDER STRATEGIES, AND CRIME PREVENTION IMPLICATIONS IN THE PHILIPPINES

Roy Villalobos, DPA, Rcrim¹, Jose Melarte G. Gooco Jr., PhD, Rcrim²,

Mildred E. Vila, PhD, PDSML, PDTQM³

Chief Engr. Ferdinand C. Villamil, PhD⁴

¹President Ramon Magsaysay State University

²President Ramon Magsaysay State University

³Philippine Christian University

⁴Philippine Christian University

Article DOI: <https://doi.org/10.36713/epra28866>
DOI No: 10.36713/epra28866

ABSTRACT

Cyber-facilitated sexual exploitation is an evolving form of technology-enabled crime that creates significant risks for children, adolescents, and other vulnerable populations. This systematic literature review examined the forms and patterns of cyber-facilitated sexual exploitation, associated risk factors, victim vulnerabilities, offender strategies, prevention and intervention measures, and crime prevention implications for the Philippines. Guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework, the study systematically searched ScienceDirect and Google Scholar for relevant literature published from 2020 to 2026. Of 172 records identified, 8 duplicates were removed, 164 records were screened, and 44 studies met the inclusion criteria and were included in the qualitative synthesis. Findings identified online grooming, online child sexual exploitation and abuse, sextortion, image-based sexual abuse, live-streamed sexual exploitation, and dissemination of child sexual abuse materials as interconnected forms of exploitation. Major vulnerabilities included poverty, family instability, previous victimization, psychological vulnerability, limited digital literacy, and inadequate supervision, while offenders commonly employed deception, manipulation, anonymity, encrypted communication, and financial coercion. Effective prevention requires integrated school-based education, family engagement, digital literacy, strengthened law enforcement and digital forensic capacity, policy measures, and multi-sector collaboration. The findings support a whole-of-society approach and inform the proposed Integrated Community Cyber Protection Framework for Philippine communities.

1. INTRODUCTION

The rapid expansion of digital technologies and internet connectivity has transformed the nature and scope of sexual exploitation, creating new opportunities for offenders to initiate, facilitate, and sustain sexually harmful behaviors across virtual environments. Cyber-facilitated sexual exploitation refers broadly to the use of information and communication technologies to perpetrate sexual abuse, coercion, manipulation, and exploitation, particularly against children and other vulnerable populations. Digital platforms enable offenders to establish contact with potential victims, cultivate trust, manipulate relationships, and sustain exploitative interactions while operating beyond traditional geographical boundaries and, in many cases, concealing their identities (Liu & Maxwell, 2026). Contemporary manifestations include online grooming, sextortion, image-based sexual abuse, live-streamed sexual abuse, online child sexual exploitation and abuse, and technology-enabled human trafficking. The accessibility,

anonymity, and persistence of digital environments allow exploitative materials to be repeatedly accessed, distributed, and monetized, while abuse may continue even without direct physical contact between offenders and victims. The permanence and replicability of digital content further intensify victimization because abusive materials may remain accessible and circulate indefinitely.

The global evidence demonstrates that cyber-facilitated sexual exploitation is both widespread and increasingly complex. Matthews et al. (2025) reported non-consensual sharing of sexual images involving children at approximately 4.9% in the United States and 7.6% in Australia, illustrating the prevalence of image-based sexual abuse among young populations. Similarly, Drejer et al. (2025) found that individuals accessing child sexual exploitation materials through dark web platforms frequently encountered live-streamed sexual abuse involving minors, demonstrating the interconnected nature of contemporary online exploitation offenses. Pereda and Otero (2026) likewise identified



elevated levels of sexual victimization among children in social welfare and residential care settings, emphasizing the particular vulnerability of marginalized populations. Beyond digital manifestations, the broader literature indicates that sexually exploited young people may experience psychological manipulation, coercive control, isolation, sexual violence, and severe physical and psychological consequences (Laird et al., 2020). These findings indicate that cyber-facilitated sexual exploitation should not be understood as a single form of cybercrime but as an evolving spectrum of interconnected forms of victimization.

The problem is particularly significant in Asia, where rapid digitalization, widespread internet access, socioeconomic inequalities, and transnational criminal networks have created conditions that can facilitate technology-enabled sexual exploitation. Southeast Asia has increasingly been identified as an important setting for online-linked exploitation. The Arakan Project (2025), as reported by the Tuos Isak Institute, identified more than 220,000 individuals as victims of online-linked exploitation associated with organized criminal operations in Myanmar and Cambodia. In Indonesia, reports have also documented the use of deceptive employment opportunities, business offers, and social media interactions to lure potential victims into exploitative situations (Tempo News Report, 2023). The use of encrypted communications and digital financial systems further complicates detection and investigation by enabling offenders and criminal networks to communicate and conduct transactions across national borders. Rocte et al. (2024) similarly noted continuing challenges among Asian countries in addressing cyber sexual exploitation facilitated through encrypted communication platforms. The Nth Room case in South Korea further illustrated how digital technologies can be exploited to blackmail victims and distribute sexually exploitative materials on a large scale. Collectively, these developments demonstrate the increasing sophistication, transnational character, and technological adaptability of cyber-facilitated sexual exploitation in Asia.

The Philippines presents a particularly important context for examining this phenomenon. The country's extensive internet and social media use, large youth population, and increasing digital connectivity provide significant opportunities for online interaction while simultaneously exposing vulnerable populations to technology-facilitated victimization. Dulanan and Bane (2024) reported that approximately 500,000 children have been trafficked or exploited through various forms of child exploitation. Filipino children and adolescents are likewise exposed to online sexual exploitation and abuse through social media and other internet-based communication channels. Evidence cited in the present review indicates that approximately 21% of online content involving children aged 12 to 17 years in 2024 contained indicators associated with online sexual exploitation and abuse. Victimization may produce consequences extending across psychological, social, economic, and interpersonal domains (Catalo-Branco et al., 2022; Harkins, 2022). Dela Rosa et al. (2023) further documented the experiences of organizations assisting women and children

victimized through trafficking and sexual exploitation in digital environments. Socioeconomic disadvantage, geographical isolation, and family circumstances may further increase vulnerability, while some documented cases have involved family members participating in the online exploitation of minors as a means of coping with economic hardship (Soco-Bautista, 2021).

Despite the growing body of research, important gaps remain in the literature. Existing studies frequently examine particular manifestations of technology-facilitated sexual exploitation—such as online sexual abuse and exploitation of children (OSAEC), online grooming, sextortion, human trafficking, and image-based sexual abuse—in isolation. Although these studies provide important insights, their fragmented focus limits a comprehensive understanding of cyber-facilitated sexual exploitation as an interconnected and evolving spectrum of technology-enabled sexual crimes. Moreover, relatively limited research has systematically synthesized evidence concerning the interaction of risk factors, victim vulnerabilities, offender strategies, prevention measures, and their implications for crime prevention. The literature also provides insufficient integration of these dimensions into a coherent framework that can guide law enforcement, victim protection, policy development, and community-based prevention. This gap is particularly important in the Philippine context, where rapidly changing digital technologies and online environments continue to create emerging opportunities for exploitation.

Accordingly, a systematic synthesis of the available evidence is necessary to consolidate current knowledge and identify patterns that may inform effective crime prevention responses. This study therefore systematically reviews the literature on cyber-facilitated sexual exploitation, with particular emphasis on its forms and patterns, associated risk factors, victim vulnerabilities, offender strategies, prevention and intervention measures, and implications for crime prevention in the Philippines. By integrating evidence from international and Philippine studies, the review seeks to provide an evidence-based foundation for strengthening prevention policies, child protection mechanisms, law enforcement responses, and multi-sector interventions addressing cyber-facilitated sexual exploitation.

2. METHODOLOGY

2.1 Research Design

This study employed a Systematic Literature Review (SLR) to synthesize existing evidence on cyber-facilitated sexual exploitation, particularly its forms and patterns, risk factors, victim vulnerabilities, offender strategies, prevention and intervention measures, and crime prevention implications relevant to the Philippine context. The review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework to promote transparency, methodological rigor, and reproducibility in the identification, screening, eligibility assessment, and inclusion of relevant literature (Page et al., 2021). Given the methodological and substantive heterogeneity of the included studies, findings were



synthesized qualitatively through thematic and narrative approaches rather than through statistical meta-analysis.

2.2 Eligibility Criteria

Eligibility criteria were established prior to the literature search to ensure consistency and relevance in study selection. Studies were included when they were peer-reviewed empirical studies using quantitative, qualitative, or mixed-methods designs and examined cyber-facilitated sexual exploitation or related forms of technology-enabled sexual victimization, including online grooming, sextortion, online child sexual exploitation and abuse (OCSEA), image-based sexual abuse, and technology-facilitated sexual violence. Eligible populations included children, adolescents, adults, vulnerable populations, offenders, practitioners, educators, law enforcement personnel, and community stakeholders. Studies published between 2020 and 2026 in English or Filipino were considered.

Studies were excluded when they consisted of editorials, opinion papers, commentaries, conference abstracts, book reviews, news articles, or other non-peer-reviewed publications; focused exclusively on offline sexual exploitation or unrelated cybercrime; involved populations unrelated to cyber-facilitated sexual exploitation; were published before 2020; or were written in languages that could not be reliably assessed by the researchers.

2.3 Information Sources and Search Strategy

A systematic literature search was conducted using ScienceDirect and Google Scholar from May 1 to May 30, 2026. These sources were selected to provide multidisciplinary literature relevant to criminology, criminal justice, psychology, sociology, information technology, public health, and the social sciences.

The search strategy was developed from the major concepts underlying the research questions and employed keywords combined through Boolean operators. The principal search terms included *cyber-enabled sexual exploitation*, *cybercrime and sexual victimization*, *human trafficking through online platforms*, *online grooming*, *online sexual exploitation*, *sextortion*, *social media-facilitated sexual abuse*, and *sexual exploitation through cybercrime in the Philippines*. These terms were searched individually and in combinations using AND and OR operators to identify literature addressing the forms of exploitation, victim vulnerabilities, risk factors, offender strategies, prevention measures, and crime prevention implications.

The principal search string was:

("cyber-enabled sexual exploitation" OR "cybercrime and sexual victimization" OR "human trafficking through online platform" OR "online grooming" OR "online sexual exploitation" OR sextortion OR "social media facilitated sexual abuse" OR "sexual exploitation through cybercrime in the Philippines")

Search results were compiled, duplicates were removed, and potentially relevant records were screened according to the predetermined eligibility criteria.

2.4 Study Selection

The study selection process followed the PRISMA 2020 framework. A total of 172 records were initially identified through database searches and other relevant sources. After removing 8 duplicate records, 164 unique records remained for title and abstract screening. Of these, 120 records were excluded because they were unrelated to the research topic, lacked relevance to the study context, or involved inappropriate populations. The remaining 44 full-text articles were assessed against the established eligibility criteria. No additional articles were excluded during the full-text eligibility assessment. Consequently, 44 studies were included in the final systematic review and qualitative synthesis.

Figure 1 presents the PRISMA 2020 flow diagram showing the identification, screening, eligibility assessment, and inclusion of studies.

2.5 Data Extraction and Synthesis

A standardized data extraction matrix was developed to systematically record information from the 44 included studies. The matrix contained twelve variables: study identification, author and year, country/setting, study design, population/sample, form of cyber-facilitated sexual exploitation, identified risk factors, victim vulnerabilities, offender strategies, prevention/intervention measures, crime prevention implications, and quality appraisal rating. The extraction framework was aligned with the objectives and research questions of the study and was used to facilitate systematic comparison of findings across the included literature.

The extracted evidence was synthesized thematically and narratively. Recurring concepts, similarities, differences, and emerging patterns were identified across studies, particularly in relation to forms of exploitation, risk factors, victim vulnerabilities, offender strategies, and prevention and intervention approaches. The synthesis subsequently informed the development of evidence-based crime prevention implications for the Philippine context.

2.6 Quality Appraisal

The methodological quality of the included studies was assessed using appraisal tools appropriate to their respective research designs. Quantitative, qualitative, experimental, mixed-methods, and cross-national studies were assessed using the Mixed Methods Appraisal Tool (MMAT), Version 2018. Systematic literature reviews and meta-analyses were assessed using AMSTAR 2, while article reviews and doctrinal/legal studies were evaluated using researcher-developed criteria addressing methodological transparency, relevance, comprehensiveness of evidence, logical consistency, and contribution to the study objectives.

Based on the applicable appraisal criteria, studies were categorized as High, Moderate, or Low quality. Quality appraisal was used to assess the strength and credibility of the available evidence and to guide interpretation of the synthesized findings. Importantly, studies were not excluded solely on the basis of their quality rating; instead, methodological quality was considered in



interpreting the evidence and developing the resulting crime prevention implications.

Among the 44 included studies, 10 were quantitative, 9 qualitative, 1 experimental, 2 mixed-methods, 1 cross-national study, 15 systematic literature reviews, and 1 meta-analysis. The MMAT 2018 was used for the first five categories, while AMSTAR 2 was used for systematic reviews and the meta-analysis.

3. RESULTS

3.1 Study Selection

The systematic search identified 172 records, consisting of 29 records from ScienceDirect and 143 from Google Scholar. After removal of eight duplicate records, 164 unique records remained for title and abstract screening. Of these, 120 records were excluded because they were unrelated to cyber-facilitated sexual exploitation, focused exclusively on offline sexual exploitation or unrelated cybercrime, involved inappropriate populations, or did not satisfy the publication criteria. The remaining 44 full-text articles were assessed for eligibility, and all 44 met the predetermined inclusion criteria. Thus, 44 studies were included in the final systematic review and qualitative synthesis.

The PRISMA selection process is summarized as follows:

PRISMA Stage	Records
Records Identified	172
Duplicate Records Removed	8
Records Screened	164
Records Excluded	120
Full-Text Articles Assessed	44
Full-Text Articles Excluded	0
Studies Included	44

The final evidence base therefore consisted of 44 studies addressing the forms, risk factors, victim vulnerabilities, offender

Study Design	n	Appraisal Tool
Quantitative	10	MMAT 2018
Qualitative	9	MMAT 2018
Experimental	1	MMAT 2018
Mixed Methods	2	MMAT 2018
Cross-National	1	MMAT 2018
Systematic Literature Review	15	AMSTAR 2
Meta-analysis	1	AMSTAR 2
Article Review	2	Researcher-developed checklist
Doctrinal/Legal Study	3	Researcher-developed checklist
Total	44	

Overall, the appraisal indicated that the included evidence demonstrated acceptable methodological rigor and was sufficient to address the objectives of the review. Studies were retained for synthesis because quality appraisal was used primarily to assess the strength and credibility of evidence rather than as an automatic exclusion criterion.

strategies, prevention and intervention measures, and crime prevention implications of cyber-facilitated sexual exploitation.

3.2 Characteristics of the Included Studies

The 44 included studies demonstrated substantial methodological and geographical diversity. The evidence base comprised 10 quantitative studies, 9 qualitative studies, 2 mixed-methods studies, 1 experimental study, and 1 cross-national study. In addition, the review included 15 systematic literature reviews, 1 meta-analysis, 2 article reviews, and 3 doctrinal/legal studies.

The studies represented multiple geographical contexts, including the Philippines, United States, United Kingdom, Australia, Canada, European countries, and other Asian settings. The populations examined included children, adolescents, young adults, adult victims, parents, educators, law enforcement personnel, practitioners, online offenders, and vulnerable communities.

Across the literature, the principal forms of cyber-facilitated sexual exploitation examined were online grooming, online child sexual exploitation and abuse (OCSEA/OSAEC), sextortion, image-based sexual abuse, technology-facilitated sexual violence, live-streamed sexual exploitation, and the production and dissemination of child sexual abuse materials.

3.3 Quality of the Evidence

The methodological quality of the included studies was assessed using design-appropriate appraisal tools. The MMAT 2018 was applied to quantitative, qualitative, experimental, mixed-methods, and cross-national studies, while AMSTAR 2 was used for systematic reviews and the meta-analysis. Article reviews and doctrinal/legal studies were assessed using researcher-developed appraisal checklists.

The distribution of studies by appraisal tool was as follows:

3.4 Forms of Cyber-Facilitated Sexual Exploitation

The thematic synthesis identified six major forms of cyber-facilitated sexual exploitation: online grooming, image-based sexual abuse, online child sexual exploitation and abuse, sextortion, live-streamed sexual abuse, and the dissemination of child sexual abuse materials. The literature indicated that these forms frequently overlap, with victims potentially experiencing



multiple forms of exploitation within the same episode or over an extended period.

Image-based sexual abuse and sextortion emerged as prominent manifestations. Offenders use intimate images or videos to threaten, coerce, manipulate, or extort victims for additional sexual content, sexual acts, or financial payments. The persistence and rapid dissemination of digital material can prolong victimization beyond the original incident (Madhu & Ramesh, 2023; Matthews et al., 2025; Pereda & Aguila-Otero, 2025).

Online grooming and OCSEA/OSAEC were likewise consistently identified. Offenders establish relationships with children and adolescents, develop trust or emotional dependence, and gradually introduce sexualized interactions or exploitative requests. The literature further linked grooming with the production and distribution of child sexual abuse materials (Ali et al., 2023; Choi & Lee, 2023; Vogt et al., 2020).

The review also identified commercial and live-streamed sexual exploitation, including coerced sexual performances, forced nudity, and live-streamed sexual abuse. These forms demonstrate the increasing commercialization and transnational character of cyber-facilitated sexual exploitation through digital communication, payment, and streaming technologies (Drejer et al., 2025; Pereda et al., 2025; Thompson et al., 2024).

3.5 Risk Factors

The findings indicate that cyber-facilitated sexual exploitation is associated with interacting individual, familial, socioeconomic, social, and technological risk factors rather than a single determinant. The most consistently reported factors were poverty and economic insecurity, family instability, previous exposure to violence or abuse, weak social protection, extensive online access, and limited digital safety awareness.

Socioeconomic disadvantage was particularly prominent. Studies identified poverty, unstable housing, financial insecurity, and limited access to basic resources as conditions that may increase vulnerability to exploitation. In some contexts, economic hardship was associated with family involvement in exploitative activities or increased susceptibility to offenders offering financial incentives (Roche et al., 2023; Pereda & Aguila-Otero, 2025).

Family dysfunction and previous victimization also emerged as important risk factors. Exposure to violence, childhood maltreatment, sexual abuse, and unstable family environments may reduce protective support and increase susceptibility to online manipulation.

Technological access further interacts with these social vulnerabilities. Social media, digital communication platforms, electronic financial systems, and other technologies increase opportunities for offenders to contact and manipulate potential victims. The literature also identified offender familiarity, trust-based relationships, and identity-related vulnerabilities as factors associated with sextortion and other forms of online sexual exploitation.

3.6 Victim Vulnerabilities

The reviewed evidence identified children and adolescents as the most consistently vulnerable populations. Developmental immaturity, dependence on adults, limited understanding of online risks, and extensive engagement with digital platforms increase their susceptibility to grooming, manipulation, and exploitation.

Other vulnerabilities included family instability, poverty, previous exposure to violence, psychological distress, social marginalization, limited digital literacy, and inadequate parental supervision. The accumulation of multiple vulnerabilities was more consistently associated with exploitation than any single demographic characteristic.

The literature also identified vulnerabilities associated with sexual minority youth and other socially marginalized populations, although the evidence indicated that victimization affects individuals across genders and age groups. The findings therefore suggest that prevention and victim-support programs should avoid narrowly defining the victim population and should recognize diverse forms of vulnerability.

Digital vulnerability was another recurring theme. Increased online exposure, inadequate parental supervision, limited knowledge of privacy and reporting mechanisms, and insufficient awareness of grooming tactics may reduce the capacity of potential victims and their guardians to identify and respond to exploitation.

3.7 Offender Strategies

The synthesis revealed that offenders employ adaptive, psychologically manipulative, and technology-enabled strategies. The most frequently identified strategies included online grooming, deception, emotional manipulation, anonymity, sextortion, financial coercion, platform migration, and the use of encrypted communication systems.

Online grooming emerged as a central strategy. Offenders gradually establish trust, emotional dependence, or perceived intimacy before introducing sexualized communication or exploitative demands. This process may progress from recruitment to manipulation, coercion, and sustained exploitation.

The literature also demonstrated that offender activity may involve organized structures rather than isolated perpetrators. These structures can include individual offenders, family-based operations, webcam exploitation establishments, and broader networks responsible for recruitment, communication, content production, and financial transactions.

Offenders also use multiple platforms to maintain access to victims and evade detection. Encrypted messaging, social media, online forums, live-streaming services, and digital financial systems can support offender collaboration, anonymity, content distribution, and financial gain.

3.8 Prevention and Intervention Strategies

The reviewed studies consistently supported a multi-level prevention approach involving schools, families, communities, law enforcement agencies, policymakers, technology companies, financial institutions, and civil society organizations. No single



intervention was identified as sufficient to address the complexity and transnational nature of cyber-facilitated sexual exploitation.

The principal prevention strategies identified were school-based cyber safety education, digital literacy, family engagement, technological safeguards, strengthened law enforcement capacity, legislative and regulatory measures, victim-centered interventions, and multi-sector partnerships.

School-based programs were particularly emphasized because they provide opportunities to develop knowledge and skills concerning online grooming, sextortion, consent, digital citizenship, and safe online behavior. Family engagement was similarly identified as an important protective mechanism through parental supervision, open communication, and awareness of online exploitation indicators.

The literature further emphasized the need for digital forensic capabilities, improved victim identification, suspicious financial transaction detection, technological detection tools, and specialized law enforcement training.

Finally, the studies highlighted the importance of government–technology sector–law enforcement–community collaboration to improve reporting mechanisms, platform safety, victim identification, information sharing, and cross-border responses.

3.9 Crime Prevention Implications for the Philippines

The thematic synthesis generated six principal crime prevention domains relevant to the Philippine context:

1. School-based cyber safety education
2. Family-centered digital guardianship
3. Digital literacy and cyber hygiene
4. Law enforcement and digital forensic capacity
5. Legislative and policy strengthening
6. Multi-sector and community partnerships

The evidence indicates that prevention should begin before victimization occurs by strengthening children's and adolescents' digital safety knowledge, improving family supervision, and establishing supportive school and community environments.

The findings further indicate a need to strengthen cybercrime investigation, digital forensics, victim identification, interagency information sharing, and legal and regulatory mechanisms. Technology providers and other stakeholders should likewise contribute to safer platform environments, effective reporting mechanisms, and measures that reduce opportunities for exploitation.

Finally, the evidence supports a whole-of-society prevention model involving government agencies, law enforcement, educational institutions, local government units, communities, technology companies, civil society organizations, and families. Such collaboration is necessary because cyber-facilitated sexual exploitation crosses institutional, geographical, and technological boundaries.

4. DISCUSSION

4.1 Cyber-Facilitated Sexual Exploitation as an Evolving Form of Crime

The findings of this systematic literature review demonstrate that cyber-facilitated sexual exploitation has evolved into a multifaceted and technology-driven form of criminality that extends beyond traditional understandings of sexual abuse. The 44 studies reviewed identified online grooming, image-based sexual abuse, online child sexual exploitation and abuse (OCSEA/OSAEC), sextortion, live-streamed sexual abuse, and the dissemination of child sexual abuse materials as interconnected manifestations of technology-enabled exploitation. Although these forms differ in execution, they share the use of digital technologies to facilitate sexual coercion, exploitation, communication, and distribution of abusive material.

The findings further indicate that digital technologies have altered the opportunity structure of sexual exploitation. Offenders can initiate contact remotely, maintain anonymity, manipulate victims over extended periods, and operate across geographical boundaries. Image-based sexual abuse and sextortion demonstrate how digital content can become a continuing instrument of coercion because material can be reproduced and redistributed rapidly. Similarly, online grooming illustrates how offenders may rely on psychological manipulation and trust-building rather than physical force.

The emergence of organized online networks is particularly significant. The reviewed literature indicates that exploitation may involve coordinated activities related to recruitment, communication, financial transactions, content production, and distribution through digital platforms. This suggests that cyber-facilitated sexual exploitation should not be conceptualized solely as an interpersonal offense between an individual offender and victim. In some circumstances, it also operates as an organized and commercially oriented cybercrime requiring digital forensic expertise, cyber intelligence, and cross-border cooperation.

This finding has important implications for the Philippine context. Although OSAEC has received substantial attention, the evidence suggests that Philippine prevention efforts must recognize the broader spectrum of cyber-facilitated sexual exploitation, including sextortion, image-based sexual abuse, online grooming, and technology-enabled sexual coercion. Such an expanded perspective is necessary to prevent emerging forms of victimization from remaining underrecognized or underreported.

4.2 Risk Factors and the Convergence of Social and Technological Vulnerability

The findings demonstrate that cyber-facilitated sexual exploitation cannot be explained by technological exposure alone. Rather, exploitation emerges from the interaction of socioeconomic, familial, psychological, and technological conditions. Poverty was consistently identified as a major vulnerability because economic insecurity can weaken protective



environments and increase susceptibility to exploitative offers and coercive relationships.

The Philippine evidence is particularly important in this regard. The literature indicates that socioeconomic disadvantage, unstable housing, unemployment, financial insecurity, and weak social protection may create circumstances in which exploitation becomes intertwined with economic survival. This suggests that crime prevention strategies focused exclusively on offender apprehension may have limited preventive impact if the structural conditions increasing vulnerability remain unaddressed.

Technology magnifies these vulnerabilities by increasing offender access to potential victims and reducing geographical barriers. Social media, digital payment systems, encrypted communication, and live-streaming platforms can be used to facilitate recruitment, communication, exploitation, and financial transactions. At the same time, the findings demonstrate that technology is not inherently criminogenic: the same technological environment can support reporting mechanisms, detection systems, content monitoring, and public education. Its preventive or harmful effects therefore depend substantially on governance, digital literacy, institutional capacity, and effective safeguards.

Family and psychological conditions further reinforce vulnerability. Family conflict, bullying, low self-esteem, emotional insecurity, and the search for acceptance may increase susceptibility to online grooming and manipulation. This reinforces the importance of addressing cyber-facilitated sexual exploitation as both a technological and social problem. Prevention must therefore strengthen not only digital safety but also family relationships, emotional resilience, social support, and child protection systems.

4.3 Victim Vulnerability: From Individual Characteristics to Cumulative Risk

The review demonstrates that children and adolescents remain particularly vulnerable because of developmental immaturity, extensive engagement with digital platforms, limited awareness of online risks, and dependence on adults for protection. However, the evidence also indicates that vulnerability cannot be reduced to age or gender. Previous victimization, psychological trauma, family dysfunction, poverty, discrimination, and social marginalization may interact to increase the likelihood of both initial victimization and revictimization.

This finding is important because it prevents victim vulnerability from being interpreted as victim responsibility. From a Victimology perspective, victimization is influenced by personal, social, and environmental conditions that may increase exposure to offenders. Lifestyle Exposure Theory further helps explain how patterns of online activity and engagement in less supervised digital environments may increase exposure to motivated offenders. These theoretical perspectives therefore support a prevention approach that strengthens protection without blaming victims for the circumstances surrounding their victimization.

The findings consequently support trauma-informed and vulnerability-sensitive prevention. Victims and potential victims

require interventions that address psychological recovery, social support, digital safety, family strengthening, and protection from revictimization. This is particularly relevant for marginalized populations whose vulnerabilities may be compounded by stigma, discrimination, poverty, and limited access to protective services.

4.4 Offender Adaptability and the Digitalization of Criminal Opportunity

The evidence indicates that offenders are increasingly adaptive in exploiting the characteristics of digital environments. Online grooming, deception, emotional manipulation, anonymity, sextortion, financial coercion, and movement across multiple platforms allow offenders to maintain access to victims while complicating detection and investigation.

This finding is consistent with Routine Activity Theory, particularly the interaction among motivated offenders, suitable targets, and the absence of capable guardianship. Digital platforms provide environments where offenders can identify and contact potential victims without needing physical proximity. Weak parental supervision, inadequate digital literacy, limited reporting mechanisms, and insufficient platform safeguards may therefore create gaps in capable guardianship.

The implication is that guardianship must be reconceptualized for digital environments. Traditional guardians such as parents, teachers, police officers, and community leaders remain important, but effective cyber guardianship also involves technology providers, platform moderators, financial institutions, cybersecurity specialists, and digital forensic investigators. Strengthening guardianship therefore requires a coordinated institutional response rather than relying on individual vigilance alone.

4.5 Prevention Requires a Shift from Reactive to Proactive Crime Prevention

A major implication of the review is that cyber-facilitated sexual exploitation cannot be effectively addressed through prosecution alone. The reviewed literature consistently supports prevention strategies involving education, digital literacy, family engagement, technological safeguards, law enforcement capacity, legislative measures, and community participation.

Situational Crime Prevention provides a useful framework for interpreting these findings because it emphasizes reducing opportunities for offending through strengthened guardianship and increased barriers to criminal activity. In the digital environment, this may involve stronger privacy protections, reporting systems, platform safeguards, age-appropriate online environments, improved detection mechanisms, and more effective digital investigation capabilities.

The findings also support the Public Health Model, which emphasizes primary prevention, risk reduction, early intervention, and the prevention of harm before victimization occurs. School-based cyber safety programs are particularly relevant because they can develop children's and adolescents' knowledge regarding grooming, sextortion, digital citizenship, consent, and safe online behavior before exploitative relationships become established.



Digital literacy should therefore be understood as a crime prevention intervention rather than simply an educational competency. Restricting internet access is neither sufficient nor sustainable in digitally connected societies. Instead, children, parents, educators, and communities require the capacity to identify manipulation, protect personal information, recognize suspicious behavior, and report exploitation safely.

4.6 The Philippine Context: Beyond OSAEC

The Philippine evidence suggests that cyber-facilitated sexual exploitation should be understood as a broader social, economic, technological, and child protection issue rather than solely as a cybercrime problem. Poverty, weak social protection, family vulnerability, digital illiteracy, and increasing technological access interact to create conditions that offenders may exploit.

The country's experience with OSAEC, particularly commercially motivated exploitation involving children, demonstrates the seriousness of the problem. However, the international literature reviewed in this study indicates that prevention must also account for online grooming, sextortion, image-based sexual abuse, live-streamed exploitation, and other technology-enabled forms of sexual coercion. The concentration of institutional attention on OSAEC may therefore leave other forms comparatively underrecognized.

This finding does not diminish the importance of OSAEC. Rather, it suggests the need for a broader conceptual and policy framework in which OSAEC is recognized as one component of a wider spectrum of cyber-facilitated sexual exploitation. Such an approach would allow Philippine crime prevention institutions to respond more effectively to emerging forms of victimization as technologies and offender strategies evolve.

4.7 Implications for an Integrated Crime Prevention Framework

The convergence of findings across the 44 studies supports an integrated prevention model rather than isolated interventions. The literature consistently points toward six mutually reinforcing domains: school-based cyber safety education, family-centered digital guardianship, digital literacy and cyber hygiene, strengthened law enforcement and digital forensic capacity, legislative and policy awareness, and multi-sector community partnerships.

These domains reflect the principle of a Whole-of-Society Approach, in which responsibility for preventing cyber-facilitated sexual exploitation is distributed among government agencies, educational institutions, families, communities, law enforcement, technology companies, financial institutions, civil society organizations, and other relevant stakeholders.

The significance of this approach lies in the interconnected nature of the crime itself. Offenders exploit technological platforms, social relationships, economic vulnerabilities, and institutional gaps simultaneously. Prevention should therefore operate across the same interconnected levels. Schools can provide early education; families can strengthen supervision and communication; communities can provide local guardianship;

law enforcement can strengthen investigation and disruption; technology providers can improve platform safety; and government can establish policy, regulatory, and social protection mechanisms.

For the Philippine setting, these findings provide an evidence-based rationale for translating systematic-review evidence into community-level crime prevention programs. The proposed Integrated Community Cyber Protection Framework (ICCPF) in the original study is consistent with this direction because it translates the synthesized evidence into interventions involving school-based cyber safety education, family digital guardianship, digital literacy and cyber hygiene, law enforcement capacity building, legislative awareness, and multi-sector partnerships.

4.8 Contribution to Criminological Knowledge and Practice

This review contributes to the criminological understanding of cyber-facilitated sexual exploitation by integrating evidence that is frequently examined separately. Rather than treating online grooming, sextortion, image-based sexual abuse, OSAEC, and live-streamed exploitation as isolated phenomena, the review demonstrates their common dependence on digital opportunity structures, victim vulnerabilities, offender adaptability, and weaknesses in guardianship.

The synthesis further demonstrates that effective crime prevention requires a movement from a predominantly reactive criminal justice orientation toward proactive, preventive, community-based, and technology-informed approaches. This does not diminish the importance of investigation and prosecution; rather, it places these functions within a broader prevention system that addresses the conditions enabling exploitation before victimization occurs.

The findings also highlight the need for continued Philippine research on comparatively underexplored forms of cyber-facilitated sexual exploitation, particularly image-based sexual abuse, online grooming, sextortion, platform-specific offending, and the effectiveness of prevention interventions.

Overall, the evidence supports the conclusion that cyber-facilitated sexual exploitation is not simply a technological crime. It is a multidimensional criminological, social, economic, child protection, and public safety problem. Consequently, sustainable prevention requires the integration of criminological theory, digital safety, social protection, education, law enforcement, technology governance, and community participation.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This systematic literature review demonstrates that cyber-facilitated sexual exploitation is a complex, evolving, and multidimensional form of crime shaped by the convergence of technological opportunities, social vulnerabilities, economic conditions, and offender adaptability. Across the 44 studies included in the review, online grooming, online child sexual exploitation and abuse, sextortion, image-based sexual abuse, live-streamed sexual exploitation, and the dissemination of child



sexual abuse materials emerged as interconnected manifestations of technology-enabled sexual exploitation.

The findings further demonstrate that victimization is rarely attributable to a single factor. Children and adolescents remain particularly vulnerable, but poverty, family instability, previous exposure to violence, psychological and emotional vulnerabilities, social marginalization, limited digital literacy, and inadequate protective supervision may interact to increase exposure to exploitation. At the same time, offenders increasingly employ deception, emotional manipulation, anonymity, encrypted communication, financial coercion, and multiple digital platforms to identify, manipulate, exploit, and control victims.

The review also establishes that effective prevention cannot rely exclusively on investigation and prosecution. Consistent evidence across the literature supports a preventive approach combining school-based cyber safety education, digital literacy, family engagement, technological safeguards, strengthened law enforcement and digital forensic capacity, legislative and policy measures, victim-centered support, and multi-sector collaboration. These findings are consistent with criminological perspectives emphasizing capable guardianship, situational opportunity reduction, vulnerability reduction, and proactive prevention.

Within the Philippine context, the findings indicate the need to broaden the understanding of cyber-facilitated sexual exploitation beyond OSAEC alone. While the protection of children remains central, emerging forms such as sextortion, image-based sexual abuse, online grooming, and live-streamed exploitation require equally sustained attention. The increasingly interconnected nature of digital platforms, financial systems, social networks, and transnational criminal activity further necessitates coordinated responses among government agencies, law enforcement, schools, families, communities, technology providers, and civil society.

Ultimately, preventing cyber-facilitated sexual exploitation requires a whole-of-society, evidence-informed, and adaptive crime prevention strategy. The study provides a consolidated evidence base for strengthening Philippine policies, institutional responses, community interventions, and future criminological research. It further provides a basis for translating systematic-review findings into practical community-based prevention initiatives through the proposed Integrated Community Cyber Protection Framework (ICCPF).

5.2 Recommendations

Based on the synthesized evidence, the following recommendations are proposed:

1. Strengthen school-based cyber safety education. Educational institutions should integrate age-appropriate cyber safety, digital citizenship, online grooming awareness, sextortion prevention, privacy protection, reporting mechanisms, and responsible online behavior into relevant educational and student-support programs. Schools should serve as an important first line of preventive education for children and adolescents.
2. Establish stronger family-centered digital guardianship.

Parents and caregivers should be provided with practical knowledge and tools for monitoring online risks, communicating with children about sexual exploitation, recognizing grooming and manipulation indicators, and responding appropriately to suspected victimization. Family interventions should emphasize supportive communication rather than punitive responses that may discourage victims from reporting.

3. Expand digital literacy and cyber hygiene programs.

Communities should receive continuing education on privacy protection, secure digital practices, suspicious online behavior, sextortion, image-based sexual abuse, and available reporting mechanisms. Digital literacy initiatives should prioritize vulnerable populations and communities with limited access to reliable cyber safety information.

4. Strengthen law enforcement and digital forensic capacity.

Relevant law enforcement agencies should continue developing specialized capabilities in cybercrime investigation, digital forensics, victim identification, online intelligence, evidence preservation, financial investigation, and cross-platform investigation. Interagency information sharing and coordination should likewise be strengthened to address the transnational and technologically adaptive nature of the crime.

5. Strengthen policy, legislative awareness, and institutional coordination.

Government institutions should continue strengthening policies and mechanisms addressing technology-facilitated sexual exploitation while ensuring that existing legal and protective measures are effectively implemented. Coordination among law enforcement agencies, social welfare institutions, educational institutions, local government units, and other relevant stakeholders should be institutionalized to improve prevention, reporting, investigation, and victim protection.

6. Increase technology-sector participation in prevention.

Technology platforms and other digital service providers should be encouraged to strengthen mechanisms for detecting exploitative activity, facilitating victim reporting, protecting users, and supporting lawful investigations. Collaboration between technology stakeholders and government institutions is particularly important because offenders can rapidly migrate across platforms and technologies.

7. Adopt a whole-of-community prevention approach.

Local governments, schools, families, community organizations, law enforcement agencies, civil society organizations, and other stakeholders should develop coordinated community-based prevention programs. Such initiatives should address both immediate digital risks and the underlying social and economic vulnerabilities associated with exploitation.

8. Translate the evidence into community-based intervention through the ICCPF.

The proposed Integrated Community Cyber Protection Framework (ICCPF) may be developed as a community-based crime prevention and extension program that integrates six evidence-informed domains: school-based cyber safety education, family digital guardianship, digital literacy and cyber hygiene, law enforcement capacity building, legislative awareness, and multi-sector partnerships.



9. Strengthen future Philippine research.

Future studies should examine comparatively underexplored forms of cyber-facilitated sexual exploitation, including image-based sexual abuse, adult online grooming, sextortion, platform-specific offending, emerging technologies, and the long-term effectiveness of prevention interventions. Philippine empirical studies should also examine the effectiveness of existing prevention and victim-support mechanisms across different geographic, socioeconomic, and institutional settings.

REFERENCES

- Ali, S., Abou Haykal, H., & Youssef, E. Y. M. (2023). *Child sexual abuse and the Internet – A systematic review*. *Human Arenas*, 6(2), 404–421. <https://doi.org/10.1007/s42087-021-00228-9>
- Aprilia, A. E., & Zainsyah, L. A. (2025). *Cybersex trafficking: Legal protection against child sexual exploitation through digital platforms*. *Veteran Law Review*, 8(2), 232–251.
- Arsawati, N. N. J. (2021). *Legal challenges of digital technology abuse in cybersex trafficking in Indonesia*. *Journal of Legal Studies and Research*, 7(3), 112–121.
- Asiyanbi, S. B., & Agboola, O. O. (2023). *Child trafficking in the digital age: The role of the dark web and cryptocurrencies in facilitating e-sexual exploitation in West Africa*. *Journal of Public Management & Information Research*, 1(2), Article 1739.
- Bag-ao, B. V. C. (2025). "In number there is strength": Multi-agency collaborative strategies for combating online sexual abuse and exploitation of children (OSAEC) in Cagayan de Oro City, Philippines. *Socialinis Darbas / Social Work*, 23(1). <https://doi.org/10.13165/SD-25-23-1-02>
- Baird, K., & Connolly, J. (2023). *Recruitment and entrapment pathways of minors into sex trafficking in Canada and the United States: A systematic review*. *Trauma, Violence, & Abuse*, 24(1), 189–202. <https://doi.org/10.1177/15248380211025241>
- Balasa Brumer, R., Khan, M., Gesink, D., Forman, L., & Perez, A. (2024). *Experiences of child sex trafficking identification among Ontario pediatric emergency department healthcare providers: A qualitative study*. *Child Abuse & Neglect*. Advance online publication. <https://doi.org/10.1016/j.chiabu.2024.106852>
- Chauwiré-Geib, K., & Fegert, J. M. (2024). *Victims of technology-assisted child sexual abuse: A scoping review*. *Trauma, Violence, & Abuse*, 25(2), 1335–1348. <https://doi.org/10.1177/15248380231178754>
- Chiu, J., & Quayle, E. (2022). *Understanding online grooming: An interpretative phenomenological analysis of adolescents' offline meetings with adult perpetrators*. *Child Abuse & Neglect*, 128, 105600. <https://doi.org/10.1016/j.chiabu.2022.105600>
- Choi, K.-S., & Lee, H. (2023). *The trend of online child sexual abuse and exploitations: A profile of online sexual offenders and criminal justice response*. *Journal of Child Sexual Abuse*, 32(8), 1007–1030. <https://doi.org/10.1080/10538712.2023.2214540>
- Christensen, L. S., & Woods, J. (2024). "It's like POOF and it's gone": The live-streaming of child sexual abuse. *Sexuality & Culture*, 28(4), 1467–1481. <https://doi.org/10.1007/s12119-023-10186-9>
- Dela Rosa, M. T. C., Lopez, S. R., & Manapol, M. L. (2023). *Experiences of female adolescents on online sexual abuse and exploitation of children during community quarantine in Davao City, Philippines*. *ASEAN Social Work Journal*, 11(1). <https://doi.org/10.58671/aswj.v11i1.46>
- Devesa, B. P. (2025). *Hashtag justice: Digital activism and the justice interests of school-related sexual violence survivors through the #HijaAko movement*. *Asian Journal of Women's Studies*. <https://doi.org/10.1080/12259276.2025.2541572>
- Drejer, C., Riegler, M. A., & Baugerud, G. A. (2025). *Live-streamed child sexual abuse: Analysis of Norwegian criminal cases*. *Child Abuse & Neglect*. Advance online publication. <https://doi.org/10.1016/j.chiabu.2025.107659>
- Dulawan, A. P., & Bance, L. O. (2024). *Deafening echoes: Lived experiences of adult survivors of online sexual abuse and exploitation of children*. *ASEAN Social Work Journal*, 12(2). <https://doi.org/10.58671/aswj.v12i2.94>
- Gaitis, K. K., Fry, D., Vermeulen, I., & Stevenson, J. G. (2025). *Extended reality environments and child safety: Examining the emerging risks for child sexual exploitation and abuse and discussing prevention and response through a technologised neo-ecological perspective*. *International Journal of Law, Crime and Justice*. Advance online publication. <https://doi.org/10.1016/j.ijlcrj.2025.100786>
- Gámez-Guadix, M., Mateos-Pérez, E., Alcázar, M. A., Martínez-Bacaicoa, J., & Wachs, S. (2024). *Stability of the online grooming victimization of minors: Prevalence and association with shame, guilt, and mental health outcomes over one year*. *Journal of Adolescence*, 96(4), 775–789. <https://doi.org/10.1002/jad.12240>
- Joleby, M., Landström, S., Lunde, C., & Jonsson, L. S. (2024). "But I wanted to talk about it": Technology-assisted child sexual abuse victims' reasoning for delayed disclosure. *Child Protection Practice*. Advance online publication. <https://doi.org/10.1016/j.chipro.2024.100062>
- Laird, J. J., Klettke, B., Hall, K., Clancy, E., & Hallford, D. (2020). *Demographic and psychosocial factors associated with child sexual exploitation: A systematic review and meta-analysis*. *JAMA Network Open*, 3(9), e2017682. <https://doi.org/10.1001/jamanetworkopen.2020.17682>
- Liu, Y. V., & Maxwell, S. R. (2026). *Perpetration and victimization of technology-facilitated sexual violence in young adults in the Philippines*. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2026.2626465>
- Lorenzo-Dus, N., Perkins, K., & Themelidis, L. (2026). "Trade?": The discourse of online sexual harmful exchanges between children. *Journal of Pragmatics*. Advance online publication. <https://doi.org/10.1016/j.pragma.2026.05.002>
- Madhu, S., & Ramesh, H. (2023). *A study on online sextortion which targets students on higher education: Bullying and cyberbullying*. In *Proceedings of the 1st International Conference on Psychology and Mental Health* (pp. 197–209).
- Mathews, B., Finkelhor, D., Collin-Vézina, D., Malacova, E., Do, H. P., & Higgins, D. J. (2025). *Characteristics of first disclosure of child sexual abuse: Age, delay, recipient, and feeling of support*. *Child Abuse & Neglect*. Advance online publication. <https://doi.org/10.1016/j.chiabu.2025.107803>
- Mathews, B., Walsh, K., Finkelhor, D., Parvin, K., Burton, M., Nicholas, M., Napier, S., Cubitt, T., de Silva, A., Higgins, D., Scott, J. G., Noll, J., & Flynn, A. (2025). *Disclosure of online child sexual victimisation: Findings from the Australian Child*



- Maltreatment Study. *Child Abuse & Neglect*, 165, 107493. <https://doi.org/10.1016/j.chiabu.2025.107493>
25. Mélody, R. L. (n.d.). The sexual exploitation of children in the digital age: An overview of a major phenomenon in Southeast Asia.
 26. Mikkola, M., Kaakinen, M., Savela, N., Oksa, R., Savolainen, I., & Oksanen, A. (2024). Cybercrime target exposure, suitability, personality, and victimization: A longitudinal approach. *Finnish Journal of Social Research*, 17, 59–76. <https://doi.org/10.51815/fjsr.144495>
 27. Moosburner, M., Weber, C., Kuban, T., Wachs, S., Schmidt, A. F., Etzler, S., & Rettenberger, M. (2025). Understanding cybergrooming: A systematic review of perpetrator characteristics, strategies, and types. *Trauma, Violence, & Abuse*. Advance online publication. <https://doi.org/10.1177/15248380251316223>
 28. Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(3–4), 303–323. <https://doi.org/10.1177/0734016820934175>
 29. Page, S., Quayle, E., McFeeters, A., Mat Rani, N. H., Slater, C., Stevenson, J., & Fry, D. (2025). Psychological and emotional harms of online child sexual exploitation and abuse in children under the age of 18: A systematic review of the evidence. *Child Abuse Review*, 34, e70048. <https://doi.org/10.1002/car.70048>
 30. Pereda, N., Águila-Otero, A., & Leiva, V. (2025). The prevalence of victimization and polyvictimization in sexual minority adolescents in Spain. *Child Abuse & Neglect*, 166, 107505. <https://doi.org/10.1016/j.chiabu.2025.107505>
 31. Pereda, N., & Águila-Otero, A. (2025). Sexual exploitation among adolescents in residential care: Prevalence and implications for child protection. *Child Abuse & Neglect*, 165, 107478. <https://doi.org/10.1016/j.chiabu.2025.107478>
 32. Proia-Lelouey, N., & Desquesnes, G. (2024). Risk factors for sex trafficking of domestic minors: An umbrella review of recent international literature. *Neuropsychiatrie de l'Enfance et de l'Adolescence*. Advance online publication. <https://doi.org/10.1016/j.neurenf.2024.10.003>
 33. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *Child Abuse & Neglect*, 110, 104355.
 34. Raines, J. (2022). Trafficking without borders: Why it is time for the law to properly address cybersex trafficking in the livestreaming context. *Catholic University Law Review*, 71, 197.
 35. Ray, A., & Henry, N. (2025). Sextortion: A scoping review. *Trauma, Violence, & Abuse*, 26(1), 138–155. <https://doi.org/10.1177/15248380241277271>
 36. Roche, S., Otarra, C., Fell, I., Torres, C. B., & Rees, S. (2023). Online sexual exploitation of children in the Philippines: A scoping review. *Children and Youth Services Review*. <https://doi.org/10.1016/j.childyouth.2023.106861>
 37. Sutton, S., & Finkelhor, D. (2024). Perpetrators' identity in online crimes against children: A meta-analysis. *Trauma, Violence, & Abuse*, 25(4), 1–13. <https://doi.org/10.1177/15248380231194072>
 38. Thompson, O. O., Aina, O. S., Idris, R. T., Ademola, E. O., Akinreti-Raji, B. A., Awange, P. D., & Oladele, S. O. (2024). "Are you gonna cooperate with me or I release your nude": Sextortion, responses and implications for national development in Nigeria. *OCHENDO: An African Journal of Innovative Studies*, 5(3).
 39. Vogt, M., Leser, U., & Akbik, A. (2020). Early detection of sexual predators in chats. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing* (pp. 3537–3546).
 40. Wood, A. C., & Wheatcroft, J. M. (2020). Young adult perceptions of Internet communications and the grooming concept. *SAGE Open*, 10(1), 1–12. <https://doi.org/10.1177/2158244020914573>
 41. Zafar, N., & Randhawa, A. A. (2021). Online sexual abuse of children, role of technology, kinds and measures for elimination. *Pakistan Journal of International Affairs*, 4(4), 124–139.