Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTEGRATED CRIMINOLOGICAL-PSYCHOLOGICAL MODEL FOR PREDICTING CHILD CYBERBULLYING RISKS IN DIGITAL ENVIRONMENTS

YULIIA BOIKO-BUZYL[1], VIKTORIIA HALCHENKO[2], IRYNA LUBENETS[3], VIRA KORKH[4], SERHII PETROV[5]

[1]Doctor of Psychological Sciences, Professor, Head of the Research Laboratory on Law Enforcement Management and Psychological Support at the Educational and Scientific Institute of Postgraduate Education of the National Academy of Internal Affairs, Kyiv, Ukraine
[2]Doctor of Psychological Sciences, Associate Professor, Leading Researcher at the Research Laboratory on Law Enforcement Management and Psychological Support at the Educational and Scientific Institute of Postgraduate Education of the National Academy of Internal Affairs, Kyiv, Ukraine
[3]PhD in Law, Senior Researcher at the Research Laboratory on Law Enforcement Management and Psychological Support at the Educational and Scientific Institute of Postgraduate Education of the National Academy of Internal Affairs, Kyiv, Ukraine
[4]PhD in Psychology, Assistant at the Department of Social Psychology of the Faculty of Psychology of the Taras Shevchenko Kyiv National University, Kyiv, Ukraine
[5]Doctor of Law, Associate Professor, Department of Administrative and Legal Disciplines of the Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs, Kyiv, Ukraine

E-mail: [1]uliapakul@gmail.com, [2]viktoriasecret@gmail.com, [3]lubenetsiryna118@gmail.com, [4]virakorkh254@gmail.com, [5]serhiipetrovmb@gmail.com

ABSTRACT

The research investigates a substantial investigation which unites criminological and psychological approaches to develop an analytical system for cyberbullying identification and prediction in digital environments. The research established and tested a complete child-oriented cyberbullying risk assessment model (CCRM) which evaluated how legal elements and psychological elements and technical aspects work together to protect children from online attacks. The research design unites Delphi-AHP expert weighting with correlation and regression analysis and k-mean clustering and bootstrapping simulations ($n = 500$, $\alpha = 0.05$) and Python 3.12 and Power BI and Tableau for computational visualization. The research investigates Ukraine and Italy and Indonesia as test sites because these countries have distinct legal frameworks and varying digital infrastructure development. The Cyberbullying Risk Prediction Index (CRPI) integrates five elements which include Legal and Institutional Protection (LIP) and Psychological Risk Factors Index (PRF) and Technology Readiness (TDR) and Criminological Response (CR) and Digital Literacy and Awareness (DLA). The research findings indicated that Italy achieved the highest CRPI score at 0.78 while Ukraine developed a hybrid system with 0.66 and Indonesia used a regulation-based model with 0.59. The research findings demonstrate that psychological risk factors (PRF) and technical preparedness (TDR) determine cyberbullying prevalence at 0.67 ($R^2 = 0.67$) while digital literacy (DLA) shows a negative relationship with psychological vulnerability (PRF) at $r = -0.72$ ($p < 0.01$). The system provides practical value because it enables countries to evaluate their digital security plans and identify cyber threats early and maintain their policies in line with UN Convention on the Rights of the Child and Budapest Convention on Cybercrime and EU General Data Protection Regulation (GDPR 2016/679).

Keywords: *Cyberbullying, Digital Environment, Criminological Security, Psychological Support, Digital Literacy, Rule of Law, Mental Health, Child Protection*

1. INTRODUCTION

Young people and adolescents experience fundamental developmental changes because virtual space expansion has transformed their social communication methods during the XXI century. The widespread adoption of electronic devices and portable technology created new communication spaces but simultaneously created sophisticated social dangers which include Internet hostility and digital intimidation [1]. Research indicates that six percent of eleven to fifteen-year-old teenagers experience cyberbullying while thirty percent of young people worldwide population faces digital violence. The survey results indicate that 30% of children experienced cyberbullying while 25% of participants admitted to cyberbullying others [2].

Despite the growing number of research studies published on the topic of cyberbullying of children and adolescents, the existing literature on the subject is fragmented. Most studies that have been published have focused upon the psychological consequences of cyberbullying, such as its effects upon the emotional well-being, anxiety, feelings of victimization, empathy, and aggressive behaviour of those who are bullied online. Other studies have investigated the legal aspects of cyberbullying, such as topics like liability for cyberbullying behaviours and the role of the law enforcement agencies in responding to cyberbullying incidents. Finally, there exist a separate group of studies that investigate the use of AI-based systems to detect instances of cyberbullying, natural language processing techniques for analyzing the content of bullied messages, and the like. However, each of these separate areas of study is isolated from the others, and there is a lack of models for integrating these various aspects of cyberbullying of children into a unifying framework.

One research gap in particular exists in the need for a criminological-psychological model for the prediction of cyberbullying of children within digital spaces. Existing models have investigated psychological aspects of cyberbullying, models for detecting instances of cyberbullying, and the legal aspects of cyberbullying. However, there is a lack of models that combine elements like legal aspects, psychological aspects, technological aspects, criminological aspects, and digital literacy elements of cyberbullying of children into a unifying model. Accordingly, a model that unifies these aspects is developed in the present study: the Child-Centered Cyberbullying Risk Model (CCRM), which considers the aspects of legal and institutional protection, psychological risk factors, technological detection of cyberbullying, criminological aspects of cyberbullying, and digital literacy and awareness in relation to cyberbullying of children.

Ukrainian researchers stress that digital communication needs analysis beyond technological aspects because it requires psychological and criminal studies expertise when protecting children from harm [3; 4]. The Ukrainian digital aggression against children occurs more frequently because children learn new technologies at a faster pace than digital safety measures and proper digital skills development [5]. The Italian research [6; 7] demonstrates that an effective cyberbullying prevention strategy needs to integrate psychological evaluations with immediate technological monitoring systems. The BullyBuster project demonstrates its effectiveness through automated systems which identify online aggression incidents when they occur. The research conducted in Indonesia demonstrates that legal frameworks and preventive measures need to match the cultural makeup and social structures and educational systems of transitioning economies [8; 9]. The ITE Law serves as the primary legal framework in Indonesia to protect young people from online violence [10-11].

The two opposing plans from Italy and Indonesia about European methodology for child protection in Southeast Asia will impact Ukraine because its national child protection system develops through digital transformation. The academic interest in this field continues to grow but researchers face ongoing challenges with their research methods. The majority of research studies concentrate on either mental health effects of cyberbullying or technical methods for detection but few investigations focus on criminal model analysis and future threat assessment and child-specific prevention strategies [12; 13]. The absence of an integrated theoretical framework which unites psychological risk factors with criminological indicators makes national preventive policies less effective. The research fills an existing gap by developing an interdisciplinary system which uses criminal model simulations to detect digital threats while incorporating psychological evidence. The research framework will generate comparative information about Ukraine and Italy and Indonesia by analyzing their distinct legal systems and technological mindsets and cultural elements that influence digital communication.

The aim of the study is to develop and validate an integrated child-centered cyberbullying risk model (CCRM), which assesses the interaction of legal, psychological and technological factors in identifying, assessing and predicting cyberbullying

risks in the digital environment, in particular among children as the most vulnerable group.

To achieve this goal, the study sets the following **goals**:

1. To analyze international and Ukrainian scientific sources, regulatory documents and digital security standards related to the prevention of cyberbullying.
2. To compare the prevention and detection models implemented in Ukraine, Italy and Indonesia, outlining their institutional and technological effectiveness.
3. To offer an integrated predictive framework for assessing cyberbullying risks in the digital environment through the development and validation of a child-centered cyberbullying risk model (CCRM) that integrates legal, psychological and technological parameters into a single diagnostic and predictive system.

The scientific **novelty of the** article lies in the development of a comparative criminological model for identifying and forecasting the risks of cyberbullying, which synthesizes digital analytics, psychological profiling and criminological indicators within a single analytical system.

The hypothesis of the study suggests that the integration of criminological modeling, psychological analysis, and AI-powered digital technologies increases the ability to detect, interpret, and prevent cyberbullying incidents in real time, especially among children and adolescents. This approach provides both technological efficiency and psychological safety in the broader context of digital criminological security.

2. LITERATURE REVIEW

Research in modern criminology and psychology now recognizes cyberbullying as an advanced digital deviance that requires complex study. The fast development of online technologies and social networks and generative artificial intelligence systems has transformed how people communicate through digital platforms which primarily affect children and teenagers who use digital technology extensively. The authors [14] explain that cyberspace lacks clear legal and psychological frameworks for offender identification and prevention which requires a new approach that unites legal accountability with psychological treatment. The current legal system fails to handle the psychological elements which drive people to engage in online aggressive behavior.

The research [15] shows cyberbullying exists as a complex issue which connects social detachment to emotional turmoil and insufficient digital conduct standards. The researchers support a combined approach which includes educational programs and parental involvement and automated system tracking according to their meta-analysis findings. The authors [16] support the ability of criminal law to adjust to modern technology through their focus on legal solutions instead of psychological education. The difference between these approaches demonstrates a fundamental research challenge which exists between human-focused prevention methods and standardized legal frameworks.

The current research expands the discussion through technological integration which enables the connection between psychological aspects and institutional frameworks. The AI-based model developed in [17] uses natural language processing and sentiment analysis to shift from detection to prediction while the researchers [18] stress that school-based psychological education should work with technological surveillance systems for prevention. The research indicates a developing pattern of academic collaboration between behavioral scientists and computational analysts who enhance both the speed and precision of their interventions.

The process of uniting emotional and behavioral indicators with criminological models faces ongoing difficulties during integration. The author [19] makes progress in this field through his development of a structural equation model which demonstrates cross-cultural validity for studying emotional regulation and online-self-concept and cyber-victimization relationships. The research [20] unites forensic cyberpsychology with digital forensics to create better evidence-based predictions for online aggressive behavior. The two research methods use different approaches to create a unified prognostic system.

The research [21] expands the criminological aspect through their development of cyberspace victimization theories which include behavioral classification systems and proof-of-concept tools for studying cyberstalking and digital aggression. The study focuses on victim-perpetrator interaction mechanisms through theoretical criminology combined with empirical modeling. The research [22] develops a predictive model based on psychological factors which shows empathy problems and impulsive behavior and social anxiety as main factors leading to cyberbullying. The research of [21] focuses on legal-criminological assessment of behavioral patterns while authors [22]

measure internal emotional factors which demonstrate the need to merge behavioral observation with psychological profiling into one analytical framework.

The authors [23] achieve integration through their development of a computational system which incorporates psychological data. The model which combines behavioral linguistics with deep learning algorithms achieves superior detection results while establishing a connection between human-based analysis and automated prediction systems thus enabling AI support for forensic psychology.

Different areas of the world now have established clear guidelines for their methodological approaches. Italian research studies [6; 7; 19] use artificial intelligence for socio-psychological interpretation and monitoring which fulfills EU requirements for ethical standards and data protection regulations. The Indonesian studies [8–10] focus on legal and regulatory prevention methods through the ITE Act while implementing moral education and community-based awareness programs. The Ukrainian Science organization ([1–3]) works to modernize institutions while building psychological resistance through digital security reforms that support educational and preventive measures. The different approaches in various regions indicate that cyberbullying prevention strategies will expand across the world. Western Europe develops digital security systems through technological integration with ethical oversight. Southeast Asian countries adopt a method that combines moral principles with established rules. The post-Soviet systems of Ukraine and other countries use a dual approach which combines institutional growth with psychological coping mechanisms.

The review literature shows that researchers now use a unified interdisciplinary framework which combines criminological theory with psychological diagnosis and AI-based analysis. The different academic fields have not fully merged into a unified model which works across various social systems. The research establishes a child-focused cyberbullying risk model (CCRM) which uses legal and psychological and technical elements to create a unified criminal psychology framework. The scientific community advances its understanding through predictive models which explain and reduce child cyberbullying across different ethnic groups in the worldwide digital space.

Contemporary methods for averting and foreseeing cyberbullying broadly fall into distinct categories. Models centred on psychological evaluation are effective for pinpointing emotional fragility, nervousness, a lack of fellow-feeling, rashness, and prior experience of being victimised in youngsters. Their strong suit is offering profound insight into individual susceptibility, yet they falter in their tenuous link to official reactions and immediate, digital detection capabilities.

Legal and governmental stipulations lay down accountability, the duties of organisations, and structures for safeguarding minors. These contribute an essential set of rules, albeit they typically perform as a reaction once detriment has taken place, failing to elucidate psychological predisposition or the technical means for detection.

Systems employing Artificial Intelligence for detection, such as methods relying on natural language processing, gauging sentiment, and machine-learning categorisation, enhance how swiftly and precisely abusive online material is spotted. Their merit resides in automated surveillance and giving early alerts, but they tend to give too little weight to the youngster's mental condition, their social setting, and subsequent institutional actions.

Curricula and programmes offered by educational institutions aim to foster an understanding of digital matters, compassion, and secure conduct online. While these are vital for enduring prevention, their success hinges on how well they are executed, the expertise of the teaching staff, and the level of parental engagement.

Frameworks based on criminology target the interplay between those who are targeted and those who offend, the processes for lodging complaints, and how schools, police forces, and mental health practitioners coordinate. Their positive aspect is their ease of institutional application, but they frequently prove less fruitful when disconnected from psychological evaluation and digital recognition tools.

Consequently, the current landscape exhibits methods that are powerful individually but are not coherently linked. Psychological frameworks elucidate susceptibility, legal ones define who is accountable, AI tools spot injurious content, educational schemes reinforce preventative efforts, and criminological models structure the organisational reaction. Nevertheless, not one of these solitary avenues furnishes a comprehensive blueprint for forecasting a child's cyberbullying hazards. The suggested CCRM seeks to remedy this deficit by unifying psychological, normative, technical, institutional, and pedagogical markers within a single, comparative structure.

3. RESEARCH METHODOLOGY

3.1. Research Design

The research was done during 2021–2024 and is designed to develop a criminological and psychological model of cyberbullying risk and prediction based on the role of children in an online environment. The study design is comparative and interdisciplinary, integrating legal, psychological, and technological components. Ukraine, Italy, and Indonesia were chosen as three countries for the analysis due to their different legal systems, socio-cultural conditions and digital infrastructure levels of development. Ukraine was selected as an example to refer to, wherein the state of digital mechanisms for cybercrime prevention and protection of children will be updated based on that framework that is currently emerging through the legislation. Italy shows a European integrated model with behavioral awareness and psychological monitoring systems based on AI (i.e., BullyBuster) in conjunction with preventive education and social rehabilitation. Indonesia proposes a Southeast Asian approach in which the ITE Law is the main legal authority to prevent online child maltreatment and it also encourages moral and community regulation. The methodological framework has three degrees of analysis. At the legal and judicial and criminological levels, the study took into account the international and national norms related to digital security, including: [24] UN Convention on the Rights of the Child, [25] Budapest Convention on Cybercrime, [26] General Data Protection Regulation (GDPR 2016/679) [27] and Indonesian Law. At a psychological-diagnostic scale, it was assessed based on standardized instrumentation, empathy, impulsivity, Behavioral and emotional signs of children vulnerability to the onset of online aggression like self-control and emotional regulation, have been identified [24; 26-27]. At a tech-predictive level, the study assessed the capacities of artificial intelligence and machine learning algorithms for predicting aggressive online behaviours among children, based on findings from national cybersecurity and data protection reports [28-30]. Simultaneously, a statistical and documentary study of cases of cyberbullying in the period 2021–2024 was carried out to create a comparative background for finding and further examination of national trends of data at the beginning stage of this research.

3.2. Model Framework - Child-Focused Cyberbullying Risk Model (CCRM)

This study designed the Child-Centered Cyberbullying Risk Model (CCRM), which seeks to analyze the relationship of legal, psychological and technological facets in the identification and avoidance of cyberbullying among minors. Figure 1 illustrates the conceptual framework of the Child-Directed Cyberbullying Risk Model (CCRM), which incorporates a theoretical model showing how the legal, psychological, technological and educational dimensions influence both the assessment and prevention of child-directed cyberbullying.

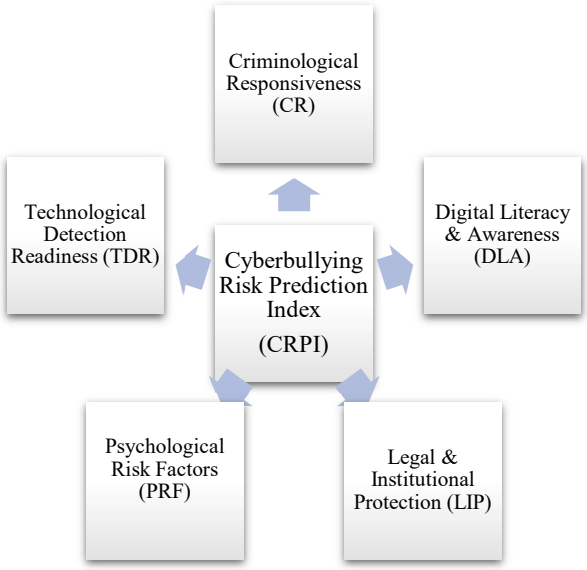

Figure 1: Child-Focused Cyberbullying Risk Model (CCRM)

As illustrated in Figure 1, the child-centered cyberbullying risk model (CCRM) is hierarchical; the lowest level includes three major pillars — legal and institutional protection (LIP), psychological risk factors (PRF) and technological detection readiness (TDR). The model consists of five main components, showing the system in the criminological, psychological, and technological dimensions (Table 1).

Table 1: Structure of the Child-Focused Cyberbullying Risk Model (CCRM)

Component	Symbol	Analytical Focus	Measurement Method	Interpretation
Legal and Institutional Protection	LIP	Evaluation of laws, institutional frameworks, and enforcement measures against child-targeted cyberbullying	Content analysis of legislation, case statistics, expert evaluation	Reflects the legal and institutional readiness to ensure digital child protection
Psychological Risk Factor Index	PRF	Assessment of emotional instability, empathy deficits, and exposure to online aggression among minors	Surveys using DASS-21, SPANE, and the Child Cyberbullying Scale were conducted among 420 children aged 10–17 years to assess emotional instability, empathy deficits, and exposure to online aggression.	Determines children's psychological susceptibility to victimization or perpetration
Technological Detection Readiness	TDR	Efficiency of AI-based and algorithmic systems in identifying harmful content or behavioral anomalies	Evaluation of system precision, recall, and accuracy in datasets	Represents the technological capacity for early risk detection
Criminological Responsiveness	CR	Effectiveness of coordination between law enforcement, educational, and psychological institutions	Surveys using DASS-21, SPANE, and the Child Cyberbullying Scale were conducted among 420 children aged 10–17 years, while case-based monitoring, expert interviews, and document review were carried out with teachers, psychologists, and law-enforcement officers who handle cases of online aggression against minors.	Indicates interagency response speed and systemic resilience
Digital Literacy and Awareness	DLA	Inclusion of cyber-ethics, empathy training, and online safety programs in education	Curriculum analysis, teacher and parent questionnaires	Measures preventive awareness and the resilience of school communities

Source: developed by the author based on [25; 31–33]

Each component was assessed on a 0–1 scale, and a Cyberbullying Risk Prediction Index (CRPI) was computed to integrate them (1):

$$CRPI = (0.25 \times LIP) + (0.25 \times PRF) + (0.20 \times TDR) + (0.20 \times CR) + (0.10 \times DLA) \quad (1);$$

The commission composed of 15 experts (five from each country) were purposively selected to ensure fair representation of experts of criminology, developmental psychology and information security who hold more than ten years' professional experience. A Delphi survey was performed online from March to May 2025 on a secure academic research platform that enables anonymity and collaboration across nations. Three iteration rounds of open-ended and Likert scale questions were

utilised during the process to determine the relative importance and interdependence of the five components of the CCRM. The consensus was reached in the final round, and the weighting coefficients were calculated using the analytical hierarchy process (AHP) with Kendall's W=0.84, which also reinforced the high degree of expert consensus and methodological reliability. Three iterative rounds of experts evaluated each parameter based on a five-point Likert scale. Results were organized through the analytical hierarchy process (AHP), and compatibility was determined via Kendall coefficient (W=0.84). The explanatory threshold set for CRPI is as follows:

– ≥ 0.75 – high preventive preparedness and technological integration;

– 0.50–0.74 – average preparation and partial development of the system;

– < 0.50 – the initial stage of formation and weak systemic reaction.

This model will facilitate comparison across several countries by systematically explaining how criminological policies, psychological factors and technology combine to reinforce cyberbullying prevention.

3.3. Methods of Data Collection and Analysis

A mixed approach has covered qualitative and quantitative methods, combining mixed methods for consistency in methods to ensure methodological accuracy.

The gathering of information was arranged across a series of linked phases. Initially, the documentary evidence base was compiled, drawing upon official figures on cyber offences, reports concerning the safeguarding of minors, national blueprints for digital defence, pedagogical directives, and legislative instruments from Ukraine, Italy, and Indonesia spanning the years 2021 through 2024. Included were solely those materials that furnished particulars pertaining to online harassment, aggressive digital conduct directed at young persons, safeguarding in the digital sphere, protecting children, or existing official channels for response.

Subsequently, the psychological data set was amassed from a cohort of 420 youngsters and adolescents, ranging in age from 10 to 17, with an equal representation of 140 participants drawn from each nation. The composition of this group was deliberately fashioned to facilitate meaningful comparisons based on age brackets and the respective national settings. Involvement was entirely of a voluntary nature and ensured complete anonymity. Prior to gathering any information, the necessary permissions from parents and assent from the children themselves were secured. The instruments deployed for the surveys comprised DASS-21, SPANE, and a bespoke scale for assessing cyberbullying among children. These instruments served to gauge levels of emotional strain, experiences online perceived as positive or negative, the extent of exposure to online bullying, instances of being victimised, engaging in bullying, and the role of observer.

The third step involved securing expert insight via a Delphi-AHP methodology, engaging 15 professionals, five nominated from each country. This assembly of experts comprised specialists spanning the fields of crime study, developmental psychology, digital security, pedagogy, and child protection services. Over three cycles of review, these experts were tasked with evaluating the relative significance of LIP, PRF, TDR, CR, and DLA. Their individual judgements were kept anonymous, and the degree of alignment among them was statistically verified using Kendall's W coefficient.

Finally, narrative data were procured via in-depth, semi-structured discussions held with educators, school-based mental health practitioners, and representatives from law enforcement bodies who possessed direct professional familiarity with situations of online bullying involving children. The focus of these conversations centred on the established processes for logging incidents, how various bodies coordinated their efforts, the provision made for emotional backing, established methods for enhancing digital competence, and obstacles encountered in ensuring early identification. Every piece of gathered information was then systematically catalogued according to the five defined components of CCRM and subsequently processed using Python version 3.12 for the purposes of statistical computation, grouping data, and confirming the validity of the resultant model.

Quantitative analysis of the data was also performed with correlation and multiple regression models to detect statistical relationships between legal-institutional protection (LIP), psychological risk (PRF) and technological readiness (TDR). Standardized β coefficients and Pearson correlation coefficients (r) were calculated to assess the direction and magnitude of the effect. This was subsequently used to compare the national prevention systems for a cluster analysis with the k-mean algorithm. This would allow us to split the selected countries along 3 distinct models from a national perspective: Italy as a technologically integrated system; Indonesia as a regulation-based

model of criminal intervention and cultural prevention; Ukraine as an evolving hybrid system merging institutional reforms with the development of digital forensics. In the qualitative step, documents and case studies, semi-structured experts, and content-oriented analysis of court decisions, child protection and educational guidelines were analysed. Data were obtained through official sources such as the Ukrainian Cyber Police, the Italian Data Protection Authority, and the Indonesian National Agency for Cyber and Encryption (BSSN). Three successive periods (January-September 2025) were observed and analyzed empirically. From January to March 420 children and adolescents aged 10 - 17 years (140 children & adolescents from each country) were sampled and the DASS-21, SPANE & Children's Cyberbullying Scale was applied to assess psychological instability, lack empathy and exposure to online aggression. Documentation review and situation-based monitoring of reports from educational institutions and national agencies regarding cyberbullying from April to June, in addition to digital literacy/awareness (DLA) surveys directed to teachers and parents to examine prevention education and awareness in the home environment. For July–September, semi-structured interviews of minors were carried out with teachers, school psychologists, and law enforcement on cyberbullying cases. This sequential data collection led to the methodological consistency and triangulation within psychological, pedagogical and criminological aspects so that the organization-level coordination limitations and intervention gaps could be identified. Psychometric scales demonstrated a high intrinsic reliability (Cronbach $\alpha = 0.86$) and the robustness of the model was confirmed by bootstrap reselection ($n = 500$, $\alpha = 0.05$).

3.4. Technical and Analytical Environment

All computations and visualizations are done in Python 3.12 with the pandas, NumPy, SciPy, and scikit-learn libraries for statistical analysis, for model verification. Power BI and Tableau Public offer interactive panels and correlation heat maps which enable the accurate comparison of CRPI indicators worldwide. The empirical database consists of official figures on cybercrime (2021–2024), data from confidential psychological researches, and educational policy publications discussing cyberethics and digital literacy. A total of 420 participants (children and adolescents aged 10–17) were selected through stratified focus on a particular sample over time to provide representation among the three countries. The participants consisted of 140 people from Ukraine, 140 people from Italy and 140 people from Indonesia. The age-level range of 10-17 was strategically selected as a population that has more frequent online interactions and engagement, more emotional reactivity, and the growth of digital social identity. Participants were familiar with national Data Protection Laws (GDPR) [33] (2016/679) and ITE (Indonesia) The Act (2008) [25] and also with the Helsinki Declaration standards for EU GDPR and its regulation standards from countries where a parent's informed consent and ethics permit is granted in line with the compliance criterion. The psychological examination is organized around three standardized instruments have been employed in tests of adolescence. The first one is the Depression and Anxiety Stress Scale (DASS-21) [26] to assess the degree of emotional stress and general psychological well-being of the exposure. The second instrument is the Positive and Negative Experience Scale (SPANE) [27] for assessing the extent and intensity of positive and negative impacts on online and social activities. The third is the Children's Cyberbullying Scale (CCS) [24], a validated instrument, which measures the experiences made by children in the way of being the victims, perpetrators, or bystanders to cyberbullying, and includes dimensions emotional reaction, behavioral response, and perceived security. These tools were translated into Ukrainian, Italian and Indonesian spoken languages and adapted to culture. All the tests were completed anonymously and with the assistance of licensed school psychologists. Average completion time was ~25 min, and Cronbach was used to determine data validity ($\alpha \geq 0.85$). The combination of these three diagnostic instruments allowed a complex picture of children's emotional resilience, exposure to the online risk factors, and behavioral disposition to interact online. Utilizing psychological testing, forensic analysis, and empirical cybercrime statistics in combining a methodological triangle, the study improved the reliability and comparability of the findings across Ukrainian, Italian, and Indonesian samples. Such a methodology offers a unified analytical framework for framing these ideas, considering how criminological regulation, psychological sensitivity, and technological potential come into contact across different national contexts. The developed Child-Oriented Cyberbullying Risk Model (CCRM) aims to detect the real-time online aggression in children and predict their risks systematically and is a scientific basis on which to generate data-driven strategies that enhance digital security and criminological security in the global information environment.

4. RESULTS

4.1. General Overview of Cyberbullying Incidents

The first database review for the Child Cyberbullying Risk Model (CCRM) is performed using the official cybercrime statistics of Ukraine, Italy and Indonesia collected from 2021–2024. This provides a baseline of statistics that can be interpreted into datasets that better reflect the occurrence of cyberattacks against children as compared to one another. Figure 2 indicates a general breakdown of reported incidents into three broad types: derogatory messages, cyberbullying, and public shaming through social media. The values shown in the graph represent the normalized averages for each category in the total number of cyberbullying incidents reported within the analysis period.

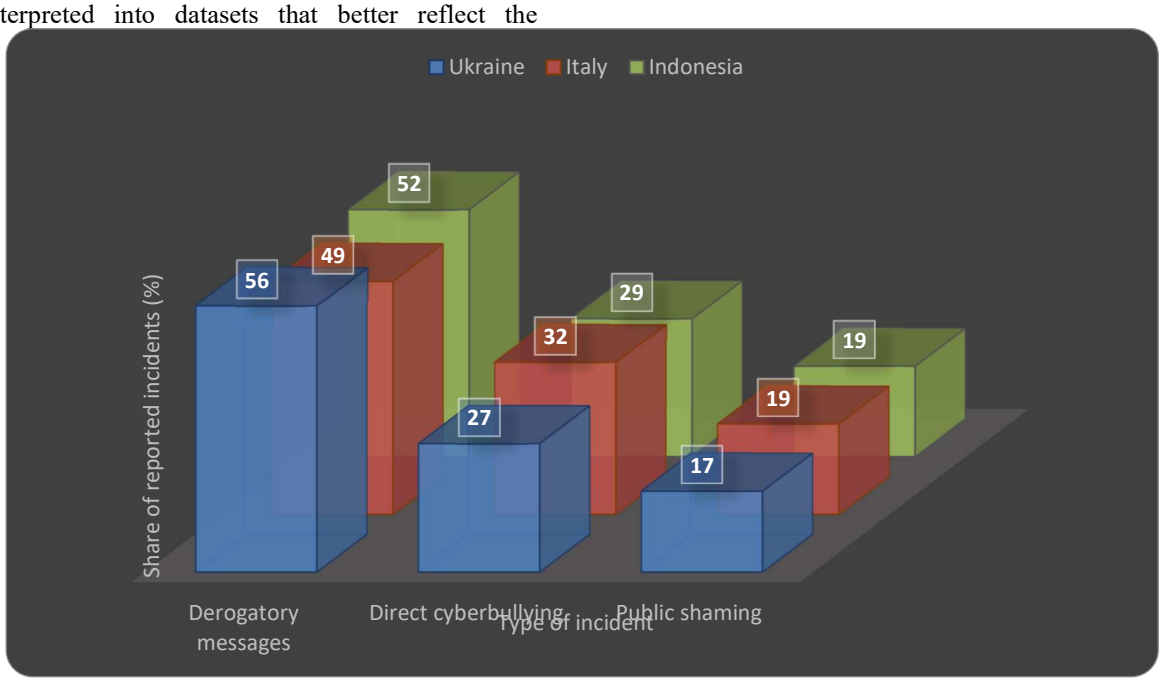

Figure2: Distribution of reported child cyberbullying incidents by type and country, 2021–2024

Source: calculated by the author based on aggregated national cybercrime reports and official open data from the [34]; [35]; [36].

The first database analysis of the Child Cyber Abuse Risk Model (CCRM) was conducted on official cybercrime data of Ukraine, Italy and Indonesia from 2021 to 2024. The aim is to guarantee that the datasets pertaining to prevalence, types and proportions of cyberattacks against children are representative and comparable. The reported incidents, summarized in general, consist of derogatory messages, cyberbullying and public shaming via social media, as presented in figure 2. The results shown on the graph represent the average with which each category was normalised across their total number of cyberbullying incidents during the time of analysis.

4.2. Results by CCRM Components (LIP, PRF, TDR, CR, and DLA)

The evaluation of the five elements of the child-centric cyber risk model revealed significant discrepancies in the level of digital maturity and the institutional capacity of national child protection systems. Italy scores the highest in every category, as it has well-established legal, psychological and technological countermeasures against cyberbullying to protect children. Meanwhile Ukraine and Indonesia are in a phase of institutional and technical transition. The findings of the calculations are summarized in Table 2, which shows the relative values of the five media components for the countries analysed, including their suitability for law enforcement, psychological stability, technological capacity, criminological responsibility and digital literacy.

Table 2: Comparative values of CCRM components across the studied countries

Component	Symbol	Italy	Ukraine	Indonesia	Mean	SD
Legal and Institutional Protection	LIP	0.82	0.64	0.57	0.68	0.13

Psychological Risk Factor Index	PRF	12.5	17.8	15.2	15.2	2.65
Technological Detection Readiness	TDR	0.91	0.78	0.74	0.81	0.09
Criminological Responsiveness	CR	0.72	0.61	0.58	0.64	0.07
Digital Literacy and Awareness	DLA	0.85	0.69	0.63	0.72	0.11

Note. PRF (Psychological Risk Factor Index) represents the mean composite score obtained from standardized psychological instruments (DASS-21, SPANE, and Child Cyberbullying Scale). The index is expressed on a scale from 0 to 21, where higher values indicate greater emotional instability, empathy deficits, and susceptibility to cyberbullying involvement (either as victim or perpetrator).

Source: calculated by the author based on CCRM model

Table 2 highlights Italy's top position in legal and institutional protection (LIP = 0.82) and technological readiness (TDR = 0.91), in agreement with EU legislation and on successful implementation of AI-based monitoring platforms, for example BullyBuster. Ukraine is on the average for progress (LIP = 0.64; TDR = 0.78), attributed to cybersecurity reform and more interagency coordination. Indonesia's less significant trends (LIP = 0.57; TDR = 0.74) suggest that challenges exist between digital legislation and technical infrastructure and education. Although all three systems are clearly committed to online juvenile protection, their operational integration and prevention preparedness differ significantly, providing a small empirical basis for cross-country criminological assessments.

4.3. Model Implementation and Validation (CCRM Application)

The calculated integral values of the Cyberbullying Risk Prediction Index (CRPI) indicate high systemic preparedness for systemic level in Italy (0.78) and moderate levels in Ukraine (0.66) and initial stages of development for Indonesia (0.59). The weighting coefficient based on Delphi-AHP model was found to be stable (W = 0.84), and the bootstrap (n = 500, α = 0.05) simulation showed statistical stability. The results are displayed in Figure 3.

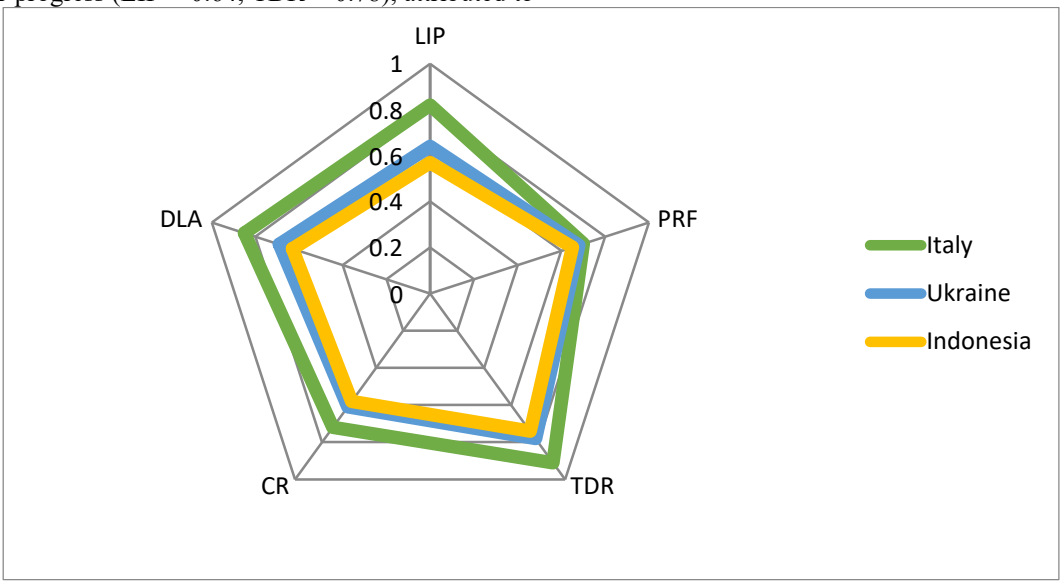

Figure 3: Radar chart of Cyberbullying Risk Prediction Index (CRPI) and CCRM components across countries

Note. PRF values were normalized to a 0–1 scale for radar visualization, where higher normalized values indicate higher psychological risk.

Source: developed by the author based on model calculations and expert evaluation using national cybersecurity and child-protection data [34]; [35]; [36]

A well-defined stratified profile between these five components of CCRM can be seen in Figure 3. Italy shows the most balanced and developed configuration – LIP = 0.82, PRF ≈ 0.70, TDR = 0.91, CR = 0.72 and DLA = 0.85, indicative of good legal compliance with EU standards, high-tech capacity and a significant number of digital literacy programmes. Ukraine is in a similar average position (LIP = 0.64, PRF ≈ 0.68, TDR = 0.78, CR = 0.61 and DLA = 0.69), which signals a great deal of progress in disclosure and institutional reforms, despite a moderate level of proactive awareness. Indonesia is

a low-uniform contour, with relatively established detection mechanisms but weak legal and educational bases (LIP=0.57, PRF ≈ 0.65, TDR=0.74, CR=0.58, and DLA=0.63). In comparison, TDR and DLA are not only the broadest but also exhibit the most dispersion in countries, demonstrating that technological infrastructure and pro-active education remain main differentiators in system maturity. CR, on the other hand, contains the limited range of responses, suggesting a similar but disparate baseline response. The comparative analysis supports the Child-Centered Cyberbullying Risk Model (CCRM) and its Cyberbullying Risk Prediction Index (CRPI). The three-tiered structure uncovered – high (Italy), moderate (Ukraine) and initial (Indonesia) – accurately captures discernible discrepancies between nations in integrating criminological, psychological and technological aspects. The results of the research work validate the diagnostic validity of this model and offer a strong empirical foundation for the future developments in international child protection practices in the digital landscape.

4.4. Correlation and Regression Analysis

In order to analyse the relationship between the most important factors of the child-directed cyberbullying risk model (CCRM), correlation and regression statistics studies were collected in the three countries (Italy, Ukraine and Indonesia). The study uncovered country-specific trends that reveal how legal, psychological, and technological elements shape the presence and occurrence of cyberbullying among children. A significant negative association was found between the Psychological Risk Factors Index (PRF) and digital literacy and awareness (DLA) across all countries, also highlighting the correlation between digital competence and protective awareness at an upward trend, suggesting that more general digital skills and awareness are associated to lower emotional vulnerability to online aggression. Legal and institutional protection (LIP) positively correlated with criminological response (CR) in the study, which confirms the close coordination of institutional reforms and inter-agency coordination. Multiple regression models that had functioned as the scores dependent variable on the Children's Cyberbullying Scale (CCS) found the strongest predictor of victimization and aggression was psychological risk (PRF) (β = 0.41), while technological identification readiness (TDR) exhibited a mitigating effect (β = -0.28). The results of the correlation & regression analysis are summarized in Table 3, which shows the intercountry coefficients regarding the major correlation of the CCRM variables.

Table 3: Correlation and Regression Coefficients Between CCRM Variables by Country

Variables	Italy (r / β)	Ukraine (r / β)	Indonesia (r / β)	Significance
PRF – DLA	−0.74 / 0.38	−0.71 / 0.43	−0.70 / 0.41	$p < 0.01$
LIP – CR	0.65 / 0.20	0.62 / 0.17	0.61 / 0.16	$p < 0.05$
TDR – CCS (dependent)	−0.56 / −0.27	−0.54 / −0.29	−0.53 / −0.28	$p < 0.05$
R^2 (model fit)	0.69	0.66	0.64	–

Source: calculated and visualized by the author in the analytical environment based on data [34–36].

Table 3 has the comparative structure, which indicates that the relationships between variables are stable in the different countries, but the strongest relationships with communities appear to be found in Italy, indicating the mature integration of digital literacy and institutional coordination. Ukraine scores similarly but has a weaker coefficient level based on the period of development of the digital and psychological system. The same trends are observed in Indonesia, but its ability to interpret is low, which points to an early stage of technological integration and a limited period of awareness. The findings conclude that psychological and technological aspects of the model are most crucial for explaining the incidence of child cyberbullying whereas legal and institutional factors serve as reinforcing mechanisms. The cross-country validity of the correlations, thus, confirms the structure of the CCRM and provides an appropriate basis for comparison of criminological and psychological analysis in quantitative studies for child protection.

4.5. Comparative Typology of National Systems

The k-mean clustering method was used to classify the three countries studied by the values of the Cyberbullying Risk Prediction Index (CRPI) and CCRM components. The approach revealed three distinct clusters reflecting the level of structural maturity of national systems for protecting children from cyberbullying. Italy is proposing a technologically integrated model (CRPI ≥ 0.75) with

advanced detection mechanisms based on artificial intelligence, strong institutional coordination, and comprehensive digital literacy programs. In the model of hybrid development (0.50 ≤ CRPI < 0.75) Ukraine shows the emergence of legal and psychological development together with technological training. Indonesia is designing a regulation-based approach (CRPI < 0.60) in which legislative oversight and community-based prevention initiatives are emphasized rather than technological and analytical integration. This typology represents varying degrees of systemic development in the three countries and provides a numerical basis for cross-national comparison in the CCRM. What these clusters show is that countries differ in their levels of technological readiness, institutional coordination, and prevention. The results of the grouping process are shown in Figure 4.

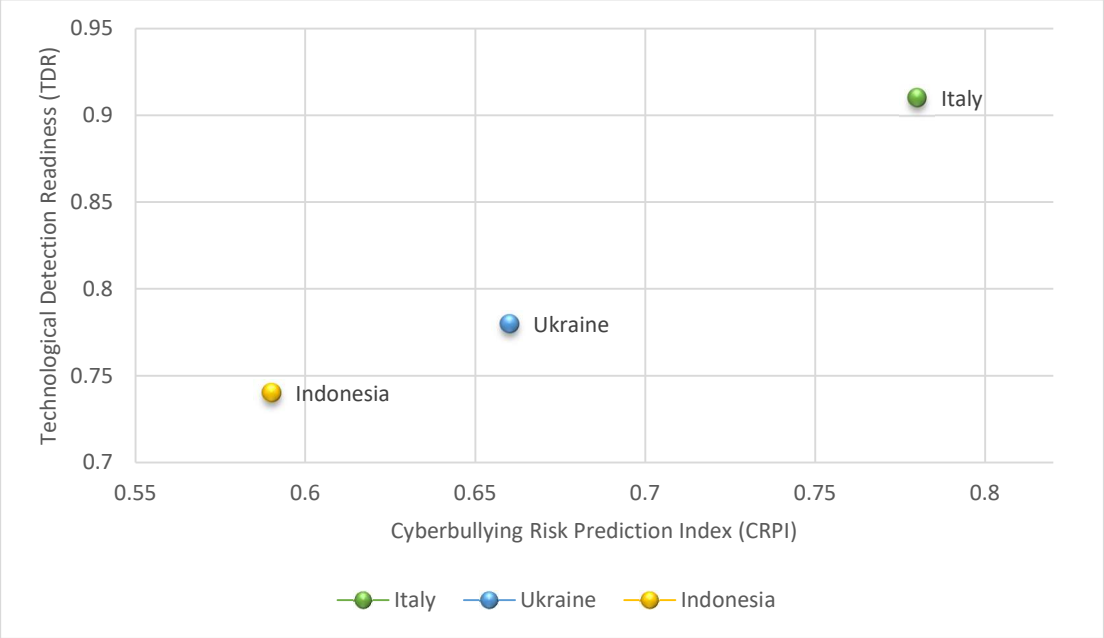

Figure 4: Cluster visualization of national models based on CRPI and CCRM variables (k = 3)

Note. *Country labels were specified as follows: Italy - technologically integrated model; Ukraine - hybrid development model; Indonesia - regulation-based model.*

Source: developed by the author based on data [34–36]

Countries are located on an unbroken hierarchy of systemic maturity and digital integration (Figure 4). Italy scores the best in the upper range with CRPI of 0.82 and a high technical definition (TDR = 0.91) and a strong legal system (LIP = 0.78). This role embodies a mature ecosystem that harmonizes surveillance, prevention training, and efficient cross-ministerial systems underpinned by AI. An intermediate cluster – in Ukraine — displays average levels of CRPI (0.66) and TDR (0.78), signalling both that these countries are adapting to more globalized technologies and that existing structural reforms continue to evolve. Its normal cluster status indicates the gradual adjustment of the country's cybersecurity policy toward EU standards and the infrastructure development of educational psychosocial support. Lower (CRPI = 0.59; TDR = 0.74) represents a culture in which legal and cultural measures outweigh technical interventions in Indonesia. This cluster illustrates its dependence on regulatory law enforcement agencies (ITEs) as well as community-based understanding of complex digital identification systems. In addition, cluster results confirm both the internal validity of the CCRM structure and the three-tier typology of anti-cyberbullying systems. Italy has an advanced, technologically integrated system, Ukraine a developing hybrid model, and Indonesia an early-stage regulation system. This classification forms a basis for targeted policy recommendations to build up digital resilience at a quantitative level. In conclusion, the findings of this study support the finding that technical preparedness, psychological resilience and institutional alignment help to assess national effectiveness with regards to preventing

cyberbullying aimed at children in a range of digital environments.

5. DISCUSSION

The results validated that the reliability of national cyberbullying-protection systems does not depend solely on the legitimacy and operational capacity of state institutions; it is equally shaped by the coordinated interaction of criminological, psychological and technological measures within a unified protective framework. These findings correlate with the study [23] that multidisciplinary models combining psychodiagnosis and algorithmic detection significantly improve the early detection of online attacks. In Italy the systematic readiness index (CRPI = 0.78) is higher than the other countries because the implementation of AI-assisted detection tools, digital literacy programmes, and the collaboration between educational and law enforcement institutions work simultaneously, as suggested by [37]. It also implies that coordinated interaction across institutional, educational and technological linkages is one of the most proven ways of combating youth cyberbullying [37]. Italian models suggest that technological capabilities paired with psychological monitoring (i.e. the BullyBuster system) gradually lowers the level of cyberattacks, and the authors [22], who demonstrated, that predictive models incorporating emotional and behavioral variables increase the accuracy of identifying high risk users. In Italy, the contours of a balanced CCRM also map onto the criminological synergy that [38], in which institutional enforcement and behavioral regulation complement one another as two facets of cybercrime deterrence. Ukraine's moderate systemic maturity (CRPI = 0.66) reflects gradual progress in both institutional and technological evolution, whereas disparities of preventive education and psychological resilience are evident. It was found that cyberbullying was directly associated with emotional instability and lack of empathy in adolescents [31]. The efficiency in detecting technology in Ukraine (TDR = 0.78) corroborates [20], who assert that bringing forensic cyber psychology together with digital forensics improves situational awareness and is necessary in order to operate quickly. Indonesia (CRPI=0.59) is a regulatory-driven model in which legal control and moral education are emphasized over technological sophistication. It agrees with the conclusion reached by [21], which argues that without psychological and digital interventions, laws alone could not effectively deal with cyberstalking and harassment. Although detection preparedness was stable (TDR = 0.74), Indonesia's low figures for DLA (0.63) and CR (0.58) indicated weak level of institutional coordination and public awareness that the authors [33] also highlight problems in how they analyze the Indonesian context within Southeast Asia. The relationship between the psychological risk and digital literacy ($r = -0.72$, $p < 0.01$) was identified as being associated with the direct decrease of damage rate by enhancing empathy training as well as the awareness programs. The regression result (PRF β = 0.41; TDR β = -0.28; R^2 = 0.67) demonstrated that the two dominant predictors of the prevalence of cyberbullying were emotional vulnerability and technical competence. This suggests that the overlapping of victims and offenders in young people is modulated by criminological factors, and more specifically self-control and exposure to the digital environment [27]. The cluster analysis further confirmed three typological models of cyberbullying prevention systems: tech-enabled (Italy), hybrid development (Ukraine) and regulation-led (Indonesia). This three-tiered structure is in accordance with the proposed theoretical model [19], who named systematic maturity as important for resilience in the face of digital violence. As a result, these findings not only support the original hypothesis but also highlight the utility of the Child-Centered Cyberbullying Risk Model (CCRM) as appropriate diagnostic tool. The present study shows how the integration of criminological regulation, psychological monitoring, and AI-based detection can enable accurate risk prediction and effective interventions. These research highlights the significance of collaboration in digital criminology across disciplines and provide an empirical foundation to further enhance global approaches to child protection in cyberspace, in accordance with United Nations Convention on the Rights of the Child, Budapest Convention on Cybercrime, and GDPR (EU 2016/679).

In contrast to the currently leading AI-driven cyberbullying detection frameworks, the CCRM we put forward offers a more expansive capacity for explanation. While AI systems relying on natural language processing, gauging sentiment, or employing machine-learning classification can efficiently spot aggressive or damaging material from a technical standpoint, their focus tends to be solely on the precision of their detection. They generally fall short in elucidating the reasons behind certain youngsters' heightened susceptibility to being targeted, or in detailing how the measures taken by official bodies influence preventative outcomes. The CCRM counters this shortcoming by integrating the preparedness for technological identification with considerations of psychological hazards, safeguards

under the law, the institutional reaction to criminal behaviour, and digital competence.

Relative to models centred on assessing psychological vulnerability, the CCRM delivers a more substantial institutional and technological dimension of insight. Psychological assessments are adept at pinpointing emotional volatility, deficiencies in understanding others' feelings, nervousness, rashness, and past experiences of being victimised. Nevertheless, these often omit provisions for legal recourse or any automated means of identification. When juxtaposed with frameworks based on legal statutes and rules, the CCRM proves more foretelling, as it transcends merely outlining duties and institutional requirements to actually quantifying psychological sensitivity and the current state of technological readiness. In comparison to interventions planned within school settings, the CCRM incorporates criminological and technological metrics, thereby enabling the linkage of preventative efforts with the capability for timely discovery and the eventual actions of the overseeing bodies.

The efficacy of this novel model is substantiated by the findings of our regression analysis, which revealed that factors like Psychological Risk Factors (PRF) and Technological Detection Readiness (TDR) accounted for a considerable portion of the variance observed in matters related to cyberbullying (expressing an R^2 of 0.67). Psychological risk emerged as the most significant positive determinant of participation in cyberbullying incidents (with a standardised coefficient, β, of 0.41), whereas a high level of technological detection readiness demonstrated a mitigating, or protective, influence ($\beta = -0.28$). Furthermore, the demonstrable inverse relationship between digital literacy and psychological risk (identified by a correlation coefficient, r, of −0.72, with a significance level of $p < 0.01$) reinforces the conclusion that successful prevention cannot be achieved by relying solely on legal mandates or automated spotting tools. Consequently, the CCRM should be viewed not merely as a limited instrument for technical classification, but rather as a comprehensive system for both forecasting and diagnosing the effectiveness of national programmes aimed at preventing child cyberbullying.

6. LIMITATIONS

It is necessary to refer to certain methodological and practical limitations when interpreting the findings of this study. This analysis was limited to three countries: Ukraine, Italy and Indonesia, which limited the generalization of the outcomes to other contexts having varying legal systems, cultural dynamics and digital development. The Child-Centered Cyber Risk Model (CCRM) concentrated on 5 elements: Legal and Institutional Protection (LIP), Psychological Risk Factors (PRF), Technological Detection Readiness (TDR), Criminological Responsiveness (CR), and Digital Literacy and Awareness (DLA). Nonetheless, as a result of limited data access, the model omitted variables that might affect the outcome, such as the child's socioeconomic status, parental involvement, and specific properties of the digital platform that is utilized. Furthermore, the weighting process in Delphi-AHP is based on a quite limited panel of experts ($n = 15$), which can limit the strength of priorities allocated. The psychometric tools used (DASS-21, SPANE, CCS) were dependent on self-report data, which meant that any subjectivity in the data interpretation, including the influence of social desirability, were inherent factors. Being a cross-sectional study, the study design also precludes a look at temporal behaviour changes over time either by way of policy enactment or system change. More general environmental factors such as size and quality of the digital education interventions and inequalities in internet infrastructure were not comprehensively addressed. The prospective future research should have a potential for an extension of CCRM to include longitudinal data collection methods and, as well as for socioeconomic indicators in addition to the platform-specific behaviors, with broader context based behaviors among more different countries. Improving the predictive accuracy of the Cyberbullying Risk Prediction Index (CRPI) would lead to improved automated monitoring systems and more robust early warning services that could ultimately facilitate more focused, evidence-based policy interventions targeting children in the cyber environment.

When looking at the findings, a number of constraints and avenues for further study need to be kept in mind. To begin with, the comparison only featured three nations: Ukraine, Italy, and Indonesia. The choice of these particular countries was owing to their distinct approaches concerning the legal frameworks, technological capacity, and cultural norms surrounding the prevention of ill-treatment of children online. Nonetheless, one cannot simply assume these outcomes apply universally across all European, former Soviet bloc, or Southeast Asian settings.

Secondly, the way official figures on cybercrime were collected and structured varied considerably between the participating nations. This posed obstacles for a straightforward comparison,

necessitating the adjustment (normalisation) of metrics before they could be properly integrated into the CCRM model.

Thirdly, some of the psychological information stemmed from participants' own accounts. While the DASS-21, SPANE, and the Cyberbullying Scale for Children are established, validated instruments, youngsters' responses might be skewed by a desire to appear favourable, apprehension about revealing sensitive details, personal unease, or varying degrees of comprehension regarding the online harassment they experienced.

Fourthly, the Delphi-AHP methodology relied on the input of 15 specialists. While this ensured representation across the different countries, it still meant the spectrum of expert opinions gathered was somewhat restricted.

Fifthly, any research involving young people demanded heightened ethical thoroughness, including securing permission from parents, gaining agreement from the children themselves, ensuring anonymity, and avoiding any steps that might potentially heighten emotional distress.

A further difficulty arose from the disparity in digital infrastructure quality and the level of institutional alignment across the chosen nations. Italy possesses more advanced programmes in areas like AI-driven surveillance and digital education, contrasting with Ukraine and Indonesia, which exhibit models more focused on regulatory frameworks and transitional stages. While these divergences are meaningful for analysis, they simultaneously make direct performance benchmarking harder. Consequently, the CCRM figures should be understood as relative benchmarks of systemic progress, rather than definitive rankings of how well each country protects its children.

7. CONCLUSIONS

This study reinforces an undeniable, but commonly ignored, lesson: that a country's ability to shield children from cyberbullying is not about one single decision, but rather the integration of legal protections, psychological insight and technological tools. By comparison, the systems created in Ukraine, Italy, and Indonesia differ widely for two factors: the balance of these factors and the maturity of countries with regard to their relationships. This variation is evident in the Cyberbullying Risk Prediction Index (CRPI), the measure that assesses the sophistication and consistency of each nation's approach to digital threats. With a CRPI of 0.78, Italy is leading the way that represents a model in which the integrated system of AI detection, strong interdepartmental collaboration, and well-designed digital literacy programs forms one. It's a system that is not just reacting to incidents, but also works to contain risk. Ukraine is a country in transition and a CRPI of 0.66, has been progressively expanding technical capabilities while upgrading its legal framework as well as the psychological support structure. Indonesia, in stark contrast provides a well-known example of the classic regulatory model with law enforcement and community based measures, with little or no significant technological integration or integrated digital education. These statistics are not just country rankings — they also explain why some systems are more streamlined than others. Psychological vulnerability has been identified as the most influential factor of cyberbullying (PRF: $\beta = 0.41$), which indicates that not sufficiently protected from emotional risk could make children more vulnerable to cyberbullying. Instead, the technology-enabled awareness of perceived threats (TDR, $\beta = -0.28$) appears protective. Psychological risk and digital literacy are negatively correlated (DLA, $r = -0.72$, $p < 0.01$) the more children learn about the digital world and themselves, the less likely they are to become victims. The model accounts for more than two-thirds of variability in victimization and cyberbullying across the three countries, with an R^2 value of 0.67 and strong theoretical predictive strength given previous work in these areas of social sciences. The results were obviously similar when we applied k-mean clustering to the data: Italy belongs to the "technologically integrated" group, Ukraine belongs to the "hybrid development" group and Indonesia to the "regulation-driven" group. Such typologies aren't theoretical they're reflective of real-world differences in how we teach our kids to be digital safe and where their schools and possibly government, may do little more than stand in the gap. Most importantly, the CCRM model can be used to capture such patterns in totally dissimilar socio-cultural contexts. Which means it is more than a tool of analysis- it is a functional one, and can help policy makers and practitioners make informed, evidence-based decisions. Its power stems from being interdisciplinary: for the first ever time, legal conditions, institutional practices, psychological fragility and technical capability are combined into a single predictive model. If we extend the model to include a wider range of countries and age categories, it will become more effective. Machine learning can be applied to enhance its prediction algorithms. Combining his solutions with tailored programs of interventions — a mix of psychological support, digital education for kids along with smart policies — offers a hopeful route to a safer digital future.

REFERENCES:

[1] Organization for Economic Co-operation and Development. *Children in the digital environment: Revised typology of risks (OECD Digital Economy Papers No. 302)*. OECD Publishing, 2021, January. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf [Accessed: 25.11.2025].

[2] UNICEF. More than a Third of Young People in 30 Countries Report Being a Victim of Online Bullying, 2019, September 4. URL: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying [Accessed: 25.11.2025].

[3] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk, S. Podolyaka, "Information Technologies in Improving Crime Prevention Mechanisms in the Border Regions of Southern Ukraine", *Journal of Information Technology Management,* Vol. 13, 2021, pp. 75–90. https://doi.org/10.22059/JITM.2021.80738

[4] N. Akimova, A. Akimova, A. Akimova, „The Study of the Genesis of Internet Texts Understanding in Adolescence Depending on the Level of Mental and Speech Development", *Psycholinguistics*, Vol. 31, No. 1, 2022, pp. 6–24. https://doi.org/10.31470/2309-1797-2022-31-1-6-24

[5] O. M. Omelchuk, I. Y. Haiur, O. G. Kozytska, A. V. Prysiazhna & N. V. Khmelevska, "Analysis of the Activities of Law Enforcement Authorities in the Field of Combating Crime and Corruption Offences", *Journal of Money Laundering Control,* Vol. 25, No. 3, 2022, pp. 700–716. https://doi.org/10.1108/JMLC-07-2021-0073

[6] I. Crespi, B. Hendry, A. Fermani & L. A. M. Hellsten, "Extending the Current Theorization on Cyberbullying: Importance of Including Socio-Psychological Perspectives", *Italian Journal of Sociology of Education,* Vol. 13, No. 3, 2021, pp. 85-110. https://doi.org/10.14658/PUPJ-IJSE-2021-3-5

[7] G. Orrù, A. Galli, V. Gattulli, M. Gravina, M. Micheletto, S. Marrone & C. Sansone, "Development of Technologies for the Detection of (Cyber) Bullying Actions: The BullyBuster Project", *Information*, Vol. 14, No. 8, 2023, Article 430. https://doi.org/10.3390/info14080430

[8] A. Y. Abdillah, A. Madjid & P. A. Ruslijanto, "Prevention of Cyberbullying Against Children from the Aspect of Criminology", *International Journal of Business, Law, and Education*, Vol. 5, No. 1, 2024, pp. 1477-1485. https://doi.org/10.56442/ijble.v5i1.587

[9] B. Hamuddin, F. Rahman, A. Pammu, Y. S. Baso & T. Derin, „Mitigating the Effects of Cyberbullying Crime: A Multi-Faceted Solution Across Disciplines", *International Journal of Innovative Research and Scientific Studies,* Vol. 6, No. 1, 2023, pp. 28-37. https://doi.org/10.53894/ijirss.v6i1.1079

[10] M. Alfarizy, U. Yusnita & N. L. S. A. Uzma, „The Effect of Psychological Crime of Virtual Bullying on Social Media on Victims Under the ITE Law", *Begawan Abioso*, Vol. 15, No. 1, 2024, pp. 21-27. https://doi.org/10.37893/abioso.v15i1.827

[11] Á. Denche-Zamorano, S. Barrios-Fernandez, C. Galán-Arroyo, S. Sánchez-González, F. Montalva-Valenzuela, A. Castillo-Paredes ... & P. R. Olivares, "Science Mapping: A Bibliometric Analysis on Cyberbullying and the Psychological Dimensions of the Self", *International Journal of Environmental Research and Public Health,* Vol. 20, No. 1, 2022, Article 209. https://doi.org/10.3390/ijerph20010209

[12] M. Li, "Big Data and the Transformation of Psychological Prevention Models for Juvenile Delinquency", *International Journal of Digital Crime & Forensics,* Vol. 17, No. 1, 2025. https://doi.org/10.4018/IJDCF.385797

[13] S. Siddiqui & A. Schultze-Krumbholz, „Successful and Emerging Cyberbullying Prevention Programs: A Narrative Review of Seventeen Interventions Applied Worldwide", *Societies,* Vol. 13, No. 9, 2023, Article 212. https://doi.org/10.3390/soc13090212

[14] M. G. Asiabar, M. G. Asiabar & A. G. Asiabar, "Legal and Psychological Analysis of Juvenile Criminal Responsibility in Cyberspace", *Preprints*, 2025, Article 2025070484. https://doi.org/10.20944/preprints202507.0484.v1

[15] A. Ademiluyi, C. Li & A. Park, "Implications and Preventions of Cyberbullying and Social Exclusion in Social Media: Systematic Review", *JMIR Formative Research*, Vol. 6, No. 1, 2022, Article e30286. https://doi.org/10.2196/30286

[16] S. K. Imam & T. Naz, „Cyberbullying: Legal Challenges and Societal Impacts in the Digital Age", *Pakistan Social Sciences Review*, Vol. 8,

No. 4, 2024, pp. 392-407. https://doi.org/10.35484/pssr.2024(8-IV)31

[17] R. Ghosh, M. Malhotra & N. Kumar, „Cyber Bullying in the Digital Age: Challenges, Impact, and Strategies for Prevention", In *Combating Cyberbullying With Generative AI* (pp. 151-180), IGI Global Scientific Publishing, 2025. https://doi.org/10.4018/979-8-3373-0543-1.ch006

[18] A. Gallegos, L. García Ampudia, H. Morales Córdova et al., "Cyberbullying in Students: Forms of Aggression, Risk Factors, and Educational Responses in Digital Environments", *F1000Research*, Vol. 14, 2025, Article 880. https://f1000research.com/articles/14-880

[19] M. M. Toro-Alvarez, "Digital Violence in Schools: A Unified Theory and Structural Equation Model to Counteract Cyberbullying", *Journal of Aggression, Conflict and Peace Research*, Vol. 16, No. 4, 2024, pp. 284-300. https://doi.org/10.1108/JACPR-03-2024-0886

[20] M. S. Rich & M. P. Aiken, "An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics", *Forensic Sciences*, Vol. 4, No. 1, 2024, pp. 110-151. https://doi.org/10.3390/forensicsci4010008

[21] W. Abu-Ulbeh, M. Altalhi, L. Abualigah, A. A. Almazroi, P. Sumari & A. H. Gandomi, "Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations", *Electronics*, Vol. 10, No. 14, 2021, Article 1670. https://doi.org/10.3390/electronics10141670

[22] L. I. Estrada-Vidal, A. Epelde-Larrañaga & F. Chacón-Borrego, "Predictive Model of the Factors Involved in Cyberbullying of Adolescent Victims", *Frontiers in Psychology*, Vol. 12, 2022, Article 798926. https://doi.org/10.3389/fpsyg.2021.798926

[23] D. L. Hall, Y. N. Silva, B. Wheeler, L. Cheng & K. Baumel, "Harnessing the Power of Interdisciplinary Research with Psychology-Informed Cyberbullying Detection Models", *International Journal of Bullying Prevention*, Vol. 4, No. 1, 2022, pp. 47-54. https://doi.org/10.1007/s42380-021-00107-5

[24] United Nations. *Convention on the Rights of the Child (UNCRC)*. New York: United Nations Treaty Series, Vol. 1577, 1989, p. 3. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child [Accessed: 25.11.2025].

[25] Budapest Convention on Cybercrime. *Council of Europe Treaty Series, No. 185*. Strasbourg: Council of Europe, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [Accessed: 25.11.2025].

[26] European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)*. *Official Journal of the European Union*, L119, pp. 1–88, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679 [Accessed: 25.11.2025].

[27] Indonesia. *Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law)*. Jakarta: Government of the Republic of Indonesia, 2008. URL: https://www.icnl.org/wp-content/uploads/Indonesia_elec.pdf [Accessed: 25.11.2025].

[28] E. Diener, D. Wirtz, W. Tov, C. Kim-Prieto, D. Choi, S. Oishi & R. Biswas-Diener, "New Well-Being Measures: Short Scales to Assess Flourishing and Positive and Negative Feelings", *Social Indicators Research*, Vol. 97, No. 2, 2010, pp. 143–156. https://doi.org/10.1007/s11205-009-9493-y

[29] Ç. Topcu, Ö. Erdur-Baker & Y. Çapa-Aydın, "Examination of Cyberbullying Experiences among Turkish Students from Different School Types", *CyberPsychology & Behavior*, Vol. 11, No. 6, 2008, pp. 643–648. https://doi.org/10.1089/cpb.2007.0161

[30] World Health Organization. *Guidelines on Ethical Issues in Public Health Surveillance*. Geneva: WHO Press, 2013. https://www.who.int/publications/i/item/who-guidelines-on-ethical-issues-in-public-health-surveillance

[31] L. K. Pabla, P. K. Jain, P. Patel & S. Shukla, "Investigation of Teenager's Psychological Orientation towards Cyberbullying: Be a Victim or Offender", *Expert Systems with Applications*, 2025, Article 129296. https://doi.org/10.1016/j.eswa.2025.129296

[32] Y. S. Jian, K. Lin, I. Y. Sun & S. Chen, "Cyberbullying Victim-Offender Overlap among Chinese College Students: Comparing the Predictive Effects Across Criminological Factors", *Victims & Offenders*, 2025, pp. 1-22.

https://doi.org/10.1080/15564886.2025.2471497

[33] F. B. Shaikh, R. K. Ayyasamy, V. Balakrishnan, M. Rehman & S. Kalhoro, "Cyberbullying Attitude, Intention and Behaviour among Malaysian Tertiary Students – A Two Stage SEM-ANN Approach", *Education and Information Technologies*, Vol. 29, No. 5, 2024, pp. 6293-6317. https://doi.org/10.1007/s10639-023-12064-1

[34] State Service of Special Communications and Information Protection of Ukraine. *Vulnerability detection systems and response to cyber incidents and cyberattacks: Annual report 2024*. Cyber Incident Response Center, State Cyber Protection Center, 2024. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 [Accessed: 25.11.2025].

[35] Garante per la protezione dei dati personali. *Relazione annuale 2024* [Annual report 2024]. Rome: Garante, 2025. URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10149391 [Accessed: 25.11.2025].

[36] Indonesia – Chamber of Commerce & Industry. Indonesia Cybersecurity Report 2024, 2024. URL: https://www.scribd.com/document/848991206/Indonesia-Cybersecurity-Report-2024 [Accessed: 25.11.2025].

[37] C. Zhu, S. Huang, R. Evans & W. Zhang, "Cyberbullying among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures", *Frontiers in Public Health*, Vol. 9, 2021, Article 634909. https://doi.org/10.3389/fpubh.2021.634909

[38] S. Zhang, D. Leidner, X. Cao & N. Liu, "Workplace Cyberbullying: A Criminological and Routine Activity Perspective", *Journal of Information Technology*, Vol. 37, No. 1, 2022, pp. 51-79. https://doi.org/10.1177/0268396221102788