

A MULTI-TIER MODEL OF SCHOOL SAFETY IN SECONDARY EDUCATION

SILVIA JAKABOVÁ, DÁŠA PORUBČANOVÁ¹, ROMAN GAWRYCH²

DOI: <https://doi.org/10.59505/IRHNS.22352007.2025.4.04>

¹DTI University,
Dubnica nad Váhom
Slovak Republic

²Wyższa Szkoła Społeczno-Ekonomiczna
Gdańsk

Contact:

PaedDr., Mgr. Silvia Jakobová, PhD. - jakabova@dti.sk
doc. PaedDr. Dáša Porubčanová, PhD. - porubcanova@dti.sk
doc. Dr. Roman Gawrych, MBA - roman.gawrych@interia.pl

Abstract:

A safe educational environment in secondary schools is a prerequisite for high-quality instruction, personal development and the mental well-being of both students and staff. In contemporary conditions, school safety can no longer be conceptualised solely through physical protection and socio-emotional climate, but must also explicitly include the digital and cyber dimension. Recent research highlights that digital transformation in education significantly increases exposure to cyber threats, disinformation and hybrid risks, which directly affect school institutions as part of the public sector. This contribution situates school safety theoretically across the physical, socio-emotional and digital dimensions, explains the

legislative framework in the Slovak Republic (SR) and the Republic of Poland (PL), and synthesises key empirical findings from domestic and international research. On the basis of this evidence, we propose a three-tier implementation model of interventions that integrates educational, organisational and cybersecurity measures and presents a practical framework for secondary school practice.

Keywords: safe educational environment; school safety; cybersecurity; resilience; wellbeing.

Introduction

Democratic societies expect schools not only to transmit knowledge but also to cultivate civic participation and to provide systematic care for the well being of their students. The debate on the safety of Slovak secondary schools intensified markedly in 2024 after several escalating incidents exposed the limits of existing protective mechanisms and created pressure for legislative change. This introductory chapter summarises key events in 2024 in Slovakia and Poland and outlines the reactions of the relevant ministries as the context from which the need for a comprehensive intervention model emerges.

Contemporary Safety Challenges in Slovak Secondary Education

A significant sense of insecurity emerged in Slovakia in May 2024, when a coordinated series of bomb threats was disseminated via e-mail to more than 1,100 public institutions, nearly 1,000 of which were primary and secondary schools. Law enforcement authorities officially classified the incident as a terrorist threat, while the Ministry of the Interior issued provisional and situational guidelines to schools, as no unified crisis-response manual had yet been established. In September, a similar pattern reoccurred in a smaller but still coordinated form, involving approximately 270 threatening e-mails. Subsequent investigations confirmed an identical modus operandi and the use of Russian internet domains, indicating a repeated and deliberate strategy.

At the same time, Slovakia experienced a notable increase in cyberattacks targeting the digital infrastructure of the Ministry of Education, alongside coordinated disinformation campaigns directed at teachers and parents. According to the analysis published by the European Digital Media Observatory (EDMO, 2024), these activities exhibited characteristics typical of hybrid

operations, combining physical intimidation with digital and informational disruption.

In response, the Ministry of Education adopted the document Crisis Events in Schools (November 2024), which for the first time systematically defined procedures for handling bomb threats, active attacker scenarios and cyber incidents, while also introducing the mandatory annual rehearsal of evacuation procedures. Shortly thereafter, the Slovak Government approved the National AI-Based Camera Project, envisaging the installation of intelligent surveillance systems in approximately 3,000 secondary schools by 2026. This initiative, however, triggered extensive public and professional debate concerning personal data protection, biometric surveillance and the proportionality of technological security measures. In parallel, a draft amendment to the Education Act was presented, obliging secondary schools to appoint a designated Safety Coordinator and to conduct an annual Safety Index audit.

The intensification of cyber-related incidents in 2024 simultaneously exposed systemic shortcomings in the digital preparedness of Slovak schools. Analyses by national cybersecurity authorities indicate that educational institutions rank among public-sector entities with comparatively low cyber resilience, frequently lacking structured staff training, formalised incident-reporting procedures and clearly defined responsibility frameworks (Bierecki et al., 2025). Consequently, the planned deployment of AI-based surveillance technologies cannot be interpreted merely as a technical security enhancement. Rather, it must be embedded within a comprehensive framework encompassing data protection policies, cybersecurity risk assessments and ethical safeguards, in alignment with European Union regulations on cybersecurity and artificial intelligence governance (Bierecki et al., 2025).

Hybrid and Digital Threats in Polish Secondary Schools: The 2024 Context

In 2024, Polish secondary schools encountered a spectrum of safety challenges comparable to those observed in Slovakia, though shaped by specific national and institutional conditions. Between May and June, a coordinated wave of hoax bomb threats was disseminated via e-mail to schools and universities in major urban centres, including Warsaw, Łódź and Rzeszów. Several incidents resulted in large-scale evacuations, notably of the University Library in Warsaw and the Łódź Academy of Music. Subsequent investigations conducted by the Internal Security Agency confirmed that the digital signatures of the threatening messages

corresponded to techniques associated with Russian military intelligence, indicating a deliberate and externally orchestrated destabilisation effort.

The security situation further escalated during the summer months following two serious violent incidents: a 17-year-old pupil carried out a knife attack against classmates in Żukowo, and an armed individual unlawfully entered a school building in Wyczółki. Although rapid police intervention prevented severe physical harm, both events exposed systemic vulnerabilities related to access control, early risk identification and the availability of psychosocial support for pupils exhibiting warning signs of distress or aggression. These incidents highlighted the limitations of existing preventive mechanisms, particularly in addressing the interaction between individual behavioural risks and institutional preparedness.

In parallel, digital threats increasingly affected the professional functioning and well-being of school staff. A nationwide survey involving 733 teachers, published at the end of 2024 in *Educational Management Administration & Leadership*, revealed that nearly half of respondents had experienced targeted online harassment, cyberbullying or coordinated digital attacks. These experiences were found to significantly undermine teachers' occupational well-being and perceived professional safety, reinforcing concerns about the growing psychological impact of digitally mediated threats within the school environment.

In response to these developments, the Ministry of National Education introduced a unified ALARM BOMB protocol, standardising procedures for verifying e-mail threats and coordinating responses with the Police and the Internal Security Agency (ABW). At the same time, the Bezpieczna+ 2.0 grant programme was expanded, with an additional allocation of PLN 42 million designated for security infrastructure improvements and digital safety training in schools. An important systemic innovation was the pilot introduction of school psychologist–crisis coordinators in ten voivodeships, complementing the provisions of the 2022 Act on the Protection of Pupils' Mental Health and strengthening schools' capacity for early intervention and crisis response.

From a broader perspective, the Polish case illustrates how the digital transformation of public institutions simultaneously enhances operational efficiency and amplifies exposure to cyber risks. As Bierecki et al. (2025) emphasise, Polish public-sector organisations—including schools—are increasingly targeted by phishing campaigns, ransomware attacks and disinformation activities conducted through online platforms. While Poland demonstrates a comparatively more advanced integration of cybersecurity considerations into national public policy than Slovakia, significant gaps remain in translating strategic frameworks

into coherent, school-level preventive and intervention practices (Bierecki et al., 2025).

Taken together, the experiences of Poland and Slovakia underline the necessity of conceptualising the safe educational environment as a dynamic and adaptive system capable of responding to cumulative physical, socio-emotional and digital threats. This shared context provides the rationale for the subsequent chapters, which elaborate the theoretical foundations of school safety, analyse the legislative frameworks of both countries, identify key determinants of a safe educational environment and propose a three-tier intervention model tailored to secondary school practice.

Theoretical Foundations

The theoretical conceptualisation of a safe educational environment (SEE) is grounded in an interdisciplinary dialogue between pedagogy, psychology and security studies. Contemporary research increasingly emphasises that school safety can no longer be understood as a static or exclusively physical condition, but rather as a dynamic and multi-layered construct shaped by interactions between organisational structures, social relationships and digital systems. In the contexts of Slovakia and Poland, this perspective is reinforced by empirical findings demonstrating that educational institutions have become exposed to hybrid constellations of physical, socio-emotional and digital risks.

Recent theoretical approaches stress the growing inseparability of educational safety and digital security. Digital transformation has fundamentally altered the boundaries of school environments, extending them into cyberspace and creating new domains in which threats may undermine institutional stability, psychological well-being and trust in public education (Bierecki et al., 2025). Against this background, the present chapter elaborates the SEE concept across three complementary dimensions - physical, socio-emotional and digital - while situating them within current theoretical frameworks and empirical evidence relevant to secondary education.

Conceptual Definitions and Core Dimensions of a Safe Educational Environment

In Slovak educational discourse, Emmerová (2024) defines a safe educational environment as “a complex set of conditions that minimises risks to health while supporting an inclusive school climate” (p. 20). A conceptually similar definition can be found in Polish pedagogical literature, where Borecka-Biernat (2022) conceptualises SEE as “a structured system protecting the physical and psychological integrity of all members of the school community” (p. 57). Despite differences in terminology, both approaches converge on a multidimensional understanding of school safety that integrates environmental, relational and organisational factors.

A shared analytical framework emerging from these definitions is the triadic structure of SEE, encompassing physical, socio-emotional and digital dimensions. The physical dimension refers to architectural design, technical safeguards and access-control measures aimed at preventing unauthorised entry and mitigating the impact of violent incidents. The socio-emotional dimension focuses on the quality of interpersonal relationships, norms and values that foster trust, inclusion and prosocial behaviour, thereby reducing both direct aggression and peer victimisation. The digital dimension reflects the exponential growth of online risks associated with digital communication, learning platforms and institutional information systems.

In recent years, the digital dimension has gained strategic importance. Bierecki et al. (2025) argue that cybersecurity should be understood as a multidimensional process involving technological safeguards, organisational preparedness and human competencies. Within the school context, this translates into the protection of digital infrastructure, the prevention of cyberbullying and disinformation, and the systematic development of digital literacy as a protective resource for pupils and teachers. Importantly, both Slovak and Polish frameworks increasingly emphasise pupil and parent participation as a dynamic element that links these dimensions and enhances institutional resilience.

The Role of Socio-Emotional School Climate in Ensuring Safety

The relationship between socio-emotional school climate and safety outcomes has been consistently confirmed by empirical research. On a Slovak sample, Hanuliaková (2008) demonstrated that schools characterised by higher levels of perceived support and fairness reported significantly lower incidences of bullying

and peer aggression. Complementary evidence from the Polish Health Behaviour in School-aged Children (HBSC) longitudinal study indicates that subjective feelings of safety are a strong predictor of adolescents' psychological well-being ($\beta = 0.32$; $p < 0.001$). These findings highlight the central role of relational trust and perceived justice in shaping pupils' experiences of school safety.

Further research underscores the preventive potential of instructional strategies that promote cooperation and shared responsibility. Wysocka (2020) found that cooperative teaching methods strengthen class cohesion and enhance pupils' willingness to intervene when witnessing violence or exclusion. Such strategies contribute to the formation of normative behaviour frameworks that discourage risk behaviour before it escalates into overt incidents.

Importantly, socio-emotional climate also moderates the impact of digital risks. Schools characterised by strong teacher–student relationships and high levels of relational trust demonstrate greater resilience to online aggression, cyberbullying and disinformation campaigns (Hanuliaková, 2021; Bierecki et al., 2025). This evidence confirms that digital safety cannot be separated from psychosocial processes operating within school communities, as supportive climates function as protective buffers against both offline and online threats.

Teacher Competence Profiles and Crisis Preparedness in Secondary Schools

Across theoretical and empirical literature, the teacher is consistently identified as a key mediator of school safety. Jablonský (2017) emphasises that teachers' abilities to manage conflicts, establish clear rules and provide emotional support substantially influence classroom climate and pupils' perceptions of safety. Polish studies by Konopczyński (2018) further demonstrate that targeted programmes aimed at developing communication and mediation skills can reduce disciplinary incidents by up to 25%. Borecka-Biernat (2022) adds that pedagogical resilience—the capacity to regulate stress and respond adaptively in crisis situations—is a significant predictor of successful implementation of school safety strategies.

Contemporary research increasingly conceptualises teacher competence as encompassing not only pedagogical and relational skills, but also digital and crisis-management capacities. Teachers represent a critical frontline in detecting cyber threats, responding to online incidents and maintaining pupils' psychological safety in digitally mediated learning environments (Bierecki et al., 2025). This expanded competence profile reflects the reality that safety-related

challenges in schools are no longer confined to physical spaces, but unfold across interconnected offline and online contexts.

However, evidence from both Poland and Slovakia points to persistent gaps in teacher preparation. Mazur (2020) highlights that faculties of education devote, on average, less than 5% of instructional time to safety-related topics, resulting in low confidence among novice teachers when confronted with crisis situations. Polish and Slovak studies converge in showing that insufficient preparation in digital risk management and crisis response contributes to elevated stress levels and reduced professional efficacy (Konopczyński, 2018; Mazur, 2020). Olejníková et al. (2025) conclude that without systematic support for teacher resilience, digital competence and legal awareness, sustainable improvements in school safety cannot be expected.

Taken together, these findings suggest that strengthening teacher competence profiles—particularly in the areas of digital safety, crisis management and socio-emotional regulation—is a prerequisite for the effective creation and maintenance of a safe educational environment in secondary schools.

School-Level Determinants of Safety: Leadership, Governance and Systemic Capacity

At the macro-school level, leadership quality and institutional governance play a decisive role in shaping safety outcomes. Transformational leadership styles are associated with clearer strategic vision, stronger staff engagement and more effective allocation of resources to preventive and protective measures. A quantitative analysis of 214 Polish secondary schools demonstrated that the quality of strategic planning was the strongest predictor of overall safety audit scores ($\beta = 0.41$; $p < 0.001$), surpassing purely technical security indicators.

Comparable tendencies have been identified in Slovakia, where schools equipped with formalised crisis-management plans and clearly defined responsibility structures show higher levels of institutional readiness. An OECD (2023) study further suggests that schools implementing systematic safety monitoring and evaluation mechanisms achieve, on average, 12% higher learning performance outcomes, supporting the assumption of a reciprocal relationship between safety and educational quality.

From a comparative perspective, studies analysing digital transformation in Poland and Slovakia highlight that systemic capacity increasingly depends on the ability of school leadership to integrate cybersecurity considerations into

organisational governance (Bierecki et al., 2025). While national cybersecurity strategies exist in both countries, their translation into school-level policies remains uneven. In contrast, Ukraine's experience—shaped by conditions of armed conflict—illustrates a more centralised and crisis-driven integration of digital security into public institutions; however, this model is not directly transferable to stable educational systems and serves primarily as a reference point for understanding the consequences of delayed preparedness.

Classroom-Level Factors: Social Structure, Climate and Digital Interaction

At the classroom level, socio-emotional climate and normative processes are critical determinants of perceived and actual safety. Classrooms characterised by mutual respect, participatory rule-setting and cooperative learning environments demonstrate lower levels of aggressive behaviour and higher collective responsibility for maintaining safety. A longitudinal study of 62 classes in four Polish regions showed that classrooms with higher levels of participatory decision-making reported 30% fewer incidents of physical bullying and 27% fewer cases of cyberbullying (Szumski, 2022).

Slovak research has long pointed to the protective function of cooperative teaching strategies. Hanuliaková (2021) demonstrated that classrooms fostering supportive peer relationships and teacher encouragement exhibit greater resilience to disruptive behaviour. These findings are reinforced by a UNESCO (2022) meta-analysis identifying teacher-mediated opportunities for participation as a key mechanism linking classroom climate to pupils' subjective sense of safety.

Recent comparative analyses further indicate that classroom climate moderates the impact of digital risks. According to Bierecki et al. (2025), digital transformation amplifies exposure to cyber aggression and disinformation, but its negative effects are significantly attenuated in environments with strong social cohesion and clear behavioural norms. Thus, classroom-level determinants operate as a bridge between institutional policies and individual experiences, translating systemic safety frameworks into everyday educational practice.

Individual level: resilience, psychological resources and contextual influences

At the individual level, pupils' perceptions of safety are closely linked to psychological resilience—the capacity to adaptively respond to stressors and to mobilise available environmental resources. A Polish survey study found that pupils with higher scores on the CD-RISC-10 resilience scale reported significantly fewer somatisation symptoms following bomb threat incidents than their less resilient peers (Mazur et al., 2024). These findings underline the importance of resilience as a protective factor buffering the psychological impact of acute safety threats.

Empirical data from Slovak pilot implementations of multi-tier safety interventions indicate that schools applying at least two layers of a three-tier model (e.g., universal and targeted interventions) recorded an 18% decrease in bullying incidents and a 7% increase in average attendance within one academic year (CPPPaP, 2024). These outcomes align with domestic findings linking positive school climate to higher learning motivation and satisfaction, as well as with international evidence supporting inclusive and high-quality secondary education.

At the same time, individual-level outcomes are shaped by broader contextual factors beyond the immediate control of schools. Multidisciplinary research suggests that social networks, digital influencers and family functioning may significantly modify the effectiveness of school-based interventions, particularly in relation to truancy and online risk behaviour. Socio-economic variables—such as local unemployment rates or community-level deprivation—continue to exert a substantial influence on both the frequency of safety incidents and educational trajectories, affecting attendance regularity, engagement and academic achievement.

The necessity of situating school safety within a wider system of societal challenges is emphasised by Pierzak and Bursová (2025), who highlight institutional adaptive capacity as a key response to environmental, economic and social crises. Similarly, Šrobárová and Bursová (2023) demonstrate that preparedness of professional teams for external stressors significantly accelerates pupils' psychological recovery following traumatic events. Although these findings partly draw on contexts of extreme crisis, they provide valuable insights for Slovakia and Poland by illustrating the long-term consequences of systemic preparedness—or its absence—on individual well-being and educational resilience.

Three-Tier Implementation Model of Interventions

The proposed three-tier intervention model operationalises the determinants of a safe educational environment identified in the preceding chapters into a structured and practically applicable framework. Conceptually, the model is rooted in Caplan's (1964) typology of prevention, which distinguishes between universal, targeted and indicated interventions. This classical framework is here reinterpreted in light of contemporary whole-school approaches to safety and well-being, including the SAMHSA Whole School Mental Health Framework (2022), the European Commission's Whole School Approach to Safety and Well-being (2023) and the WHO guidelines on school mental health (2023).

Unlike fragmented or reactive safety measures, the three-tier model is designed as an integrated system that aligns organisational governance, classroom practices and individual support mechanisms. Its core strength lies in the coordination of intervention levels, allowing schools to address everyday risks preventively while maintaining the capacity to respond effectively to acute or individualised safety threats. The model is therefore adaptable to the institutional conditions of secondary schools in Slovakia and Poland, while remaining sensitive to broader regional experiences.

Universal Interventions: Building Shared Norms and Preventive Capacity

Universal interventions form the foundation of the model and are directed at the entire school community. Their primary function is to establish shared behavioural norms, strengthen institutional culture and reduce the likelihood of safety incidents through preventive action. International evidence consistently shows that schools investing in whole-school preventive strategies achieve not only lower rates of disciplinary incidents but also improved educational outcomes.

Rather than replicating specific programmes, the universal tier of the present model emphasises transferable principles: clarity of rules, consistency of enforcement, and active participation of pupils and staff in shaping school norms. Comparative analyses of international initiatives such as PBIS and KiVa demonstrate that when prevention is embedded into everyday school routines, it produces sustained reductions in problem behaviour and enhances pupils' sense of belonging (Horner & Sugai, 2023).

In the Slovak and Polish contexts, the universal tier integrates a clearly articulated zero-tolerance stance towards violence, a systematically embedded

media and digital literacy curriculum addressing misinformation and online risks, and participatory structures such as school parliaments or class councils. These mechanisms foster shared responsibility for safety and strengthen collective resilience without overburdening schools with externally imposed programme requirements.

Targeted Interventions: Differentiated Support for At-Risk Groups

The targeted level addresses classes or groups of pupils who exhibit elevated risk indicators, such as recurring conflicts, low cohesion or early signs of disengagement. Interventions at this level are selective rather than universal and aim to interrupt negative trajectories before they escalate into serious safety incidents.

Evidence from European practice indicates that group-based interventions focusing on social competence, emotional regulation and peer support can significantly reduce aggressive behaviour and improve classroom climate. Within the proposed model, the targeted tier includes structured resilience-building activities, peer mentoring schemes and short-term psychoeducational modules implemented in classes with unfavourable Safety Index profiles.

Crucially, targeted interventions function as a bridge between preventive school-wide strategies and individualised care. By responding flexibly to emerging risks, they reduce the pressure on tertiary services and contribute to a more efficient allocation of professional support resources within the school system.

Indicated Interventions: Individualised and Crisis-Oriented Responses

Indicated interventions are designed for pupils who have been identified as facing high or acute risk, including exposure to violence, severe psychological distress or credible threat-related behaviour. At this level, the emphasis shifts from prevention to protection and recovery.

In both Slovakia and Poland, recent legislative developments underscore the growing importance of multidisciplinary responses involving school psychologists, external specialists and, where necessary, law enforcement agencies. The present model integrates individual crisis counselling, structured threat-assessment procedures and post-incident psychological debriefings as core

components of the indicated tier.

Rather than treating individual cases in isolation, the model situates indicated interventions within the broader school safety ecosystem. This ensures continuity between immediate crisis response and longer-term reintegration of pupils into the educational process, thereby minimising secondary harm and stigmatisation.

Implementation Fidelity and Evaluation Frameworks

Research on school-based interventions consistently demonstrates that effectiveness depends not only on programme design but also on implementation fidelity—that is, the extent to which prescribed procedures are applied as intended. Variability in implementation quality can significantly weaken otherwise evidence-based interventions.

To address this risk, the model incorporates explicit mechanisms for monitoring and evaluation. These include the appointment of school safety coordinators, the use of structured checklists and periodic self-assessments, and the integration of quantitative indicators into a digital Safety Index dashboard. External supervision and annual review cycles further support reflective practice and continuous improvement, reinforcing institutional learning rather than punitive accountability.

Comparative Analysis of Selected School Safety Intervention Models

The table below situates the proposed model within a broader comparative context. Ukraine is included solely as a reference case, illustrating outcomes observed under conditions of prolonged systemic stress and crisis, and not as a directly transferable model for Slovakia or Poland.

Table 1 International School Safety Frameworks Comparison

Model / Framework	Country	Core outcomes (2022–2024)	Implementation load	Applicability to SR/PL	Reference note: Ukraine
PBIS	USA	– 20% disciplinary referrals; + 13% academic performance	Medium	High	Not applicable
KiVa	Finland	– 30% bullying; + 11% pupil satisfaction	High (licensed)	Moderate	Not applicable
eSafety Schools	Australia	+ 41% cyber incident reporting; – 18% cyberbullying	Medium	High	Not applicable
TaMHS 2.0	UK	+ 25% SDQ well-being scores	Low	High	Not applicable
Bezpieczna+ 2.0	Poland	– 18% disciplinary recidivism	Low	High	Not applicable
Crisis-integrated school safety (reference)	Ukraine	Rapid crisis response; high reliance on external coordination	Very high	Low (context-specific)	Illustrative of extreme-system stress

Added Value and Practical Implications of the Three-Tier Model

By integrating universal, targeted and indicated interventions into a coherent framework, the three-tier model enhances the stability and predictability of school safety practices. For school leadership, it provides a strategic structure that links prevention, response and evaluation. For teachers, it offers clear procedural guidance and institutional support, reducing role overload and stress. Pupils benefit from improved well-being, stronger engagement and reduced exposure to risk behaviours.

At the societal level, the model contributes to long-term benefits by lowering indirect costs associated with school violence, dropout and mental health problems. Schools that succeed in maintaining a safe educational environment strengthen public trust in education and foster social capital by preparing graduates who demonstrate higher levels of civic responsibility and resilience.

Discussion

This contribution argues that a safe educational environment in secondary schools must be conceptualised and operationalised as a multidimensional, adaptive system rather than as a set of isolated protective measures. The evidence and contextual developments presented across Chapters 1–4 indicate

that the traditional emphasis on physical safeguards and socio-emotional climate - although still necessary - has become insufficient under contemporary conditions. The escalation of hybrid threats in 2024 in both Slovakia and Poland, including coordinated e-mail intimidation, disinformation activity and increasing cyber incidents targeting public-sector institutions, demonstrates that the boundaries of school safety have expanded decisively into the digital domain (EDMO, 2024; Bierecki et al., 2025). Consequently, safe educational environment must be understood as an interdependent structure in which physical security, psychosocial processes and cybersecurity governance mutually condition each other.

Reconceptualising the Safe Educational Environment: From Protection to Systemic Resilience

A key discussion point emerging from the text is the need to move from a reactive interpretation of school safety toward a resilience-oriented paradigm. The Slovak response—particularly the introduction of the Crisis Events in Schools guidance (November 2024), annual evacuation rehearsals and the planned AI-based surveillance project—illustrates that crisis-driven events accelerate policy action, yet simultaneously raise ethical and governance questions. The Slovak Spectator, 4 September 2024). In Poland, the ALARM BOMB protocol and the expansion of Bezpieczna+ 2.0 similarly indicate a shift toward formalisation and standardisation of procedures. However, the discussion must emphasise that standardisation alone does not guarantee resilience. The concept of resilience requires that institutions possess not only procedures, but also the organisational capacity and human competences to implement them consistently across everyday school functioning.

The comparative framing presented suggests that Slovakia and Poland are converging in recognising SEE as a dynamic construct; nonetheless, both systems face a similar challenge: translating national-level policy intentions into coherent school-level practice. This gap is particularly visible in the digital domain, where schools are increasingly exposed to phishing, ransomware and disinformation, while their internal incident-reporting routines, responsibility structures and staff training remain uneven (Bierecki et al., 2025). The discussion therefore supports the argument that SEE should be treated as a governance issue—embedded in school leadership, organisational planning and evaluation—rather than only as a security hardware problem.

Digital Safety as an Integral Structural Component of Educational Safety

One of the most consequential implications of the presented material is that digital security can no longer be framed as an “additional” safety topic or as a matter of individual ICT competence. Bierecki et al. (2025) conceptualise cybersecurity as a multidimensional process combining technological safeguards, organisational preparedness and human competencies, which aligns with the paper’s triadic SEE structure. Within schools, the digital dimension introduces risks that differ qualitatively from traditional threats: they are scalable, anonymous, persistent and often psychologically invasive. The nationwide data referenced in Poland—where nearly half of teachers reported targeted online harassment or cyberbullying—supports the interpretation that digital threats increasingly affect staff occupational well-being and perceptions of safety, not merely student behaviour (Bierecki et al., 2025).

In this context, the planned expansion of AI-based surveillance in Slovakia should be interpreted not as a standalone security intervention, but as one element within a broader governance package that must include privacy safeguards, proportionality principles and cybersecurity risk management consistent with EU policy frameworks (Bierecki et al., 2025). The discussion thus underscores a crucial point: schools can inadvertently increase risk if technological measures are introduced without parallel investments in data protection, ethical oversight, and staff capacity to manage incidents. Safety, in this framing, is co-produced by technology, institutional routines and professional judgement.

Socio-Emotional School Climate as a Moderator of Digital Risks

Chapters 2 and 3 allow an important interpretive conclusion: socio-emotional climate is not merely a parallel dimension to digital safety but functions as a moderating mechanism that shapes vulnerability and resilience to online harms. The Slovak evidence that supportive climates are associated with lower bullying incidence (Hanuliaková, 2021), together with the Polish HBSC findings linking perceived safety to adolescent well-being, supports the claim that relational trust and perceived justice are foundational protective resources. Importantly, these resources operate across both offline and online interaction contexts.

The discussion therefore argues that school safety interventions cannot be segmented into “digital” versus “psychosocial” packages. Instead, strong teacher–student relationships, consistent rule enforcement and participatory norm formation create a social infrastructure that buffers the effects of cyberbullying

and disinformation, while weak climates amplify their impact (Bierecki et al., 2025). This also helps explain why schools that invest in cooperative strategies and participatory decision-making report reductions in both physical and cyberbullying (Szumski, 2022). In practice, this implies that digital safety is partially achieved through “non-digital” means: classroom cohesion, fairness and predictable behavioural norms.

Teacher Competence and Preparedness as a Critical Systemic Vulnerability

A recurring theme across the text is that teacher preparedness functions as a bottleneck variable for SEE implementation. Theoretical framing positions teachers as key mediators of classroom safety and emotional regulation (Jablonský, 2017), while Polish evidence indicates that communication and mediation programmes can reduce disciplinary incidents substantially (Konopczyński, 2018). Yet the discussion must confront the structural reality highlighted by Mazur (2020): teacher education devotes only a limited share of instructional time to safety-related competencies, contributing to low efficacy in crisis situations and digital risk management.

This gap becomes more critical under hybrid threat conditions because teachers operate as first responders within schools: they detect early warning signs, enforce rules, manage escalation, and provide psychological support in the immediate aftermath of incidents. Bierecki et al. (2025) strengthen this argument by showing that organisational and human factors shape cyber resilience in public institutions. Thus, even well-designed legal frameworks and protocols may fail if teachers are not supported through systematic training in crisis response, digital safety, and legal responsibilities. Olejníková et al. (2025) further reinforce that resilience-building is not optional, but a prerequisite for sustainable safety improvement.

The implication is that SEE reform cannot rely primarily on external security inputs (technology, police coordination, protocol documents). It must include the internal professionalisation of staff through sustained and practice-oriented development focused on behavioural management, digital incident response and psychosocial support.

Multilevel Determinants of School Safety: Rationale for a Tiered Intervention Model

The determinants presented in Chapter 3 support a multilevel interpretation of SEE. At the macro-school level, strategic planning and leadership predict safety audit outcomes and align with international evidence that formal crisis planning correlates with improved learning performance (OECD, 2023; Woynarowska, 2023). At the classroom level, participation and cohesion reduce bullying and cyberbullying (Szumski, 2022), while at the individual level, psychological resilience buffers stress impacts and supports continuity of schooling even under threat exposure (Mazur et al., 2024). Together, these results justify the paper's central methodological decision: proposing a three-tier intervention model that coordinates universal, targeted and indicated measures (Caplan, 1964).

The discussion therefore frames the three-tier model not as a prescriptive programme, but as a logic of alignment: universal measures create baseline norms and preventive capacity; targeted measures address emerging group-level risk patterns; and indicated measures provide individualised protection and recovery. Importantly, this tiered structure also reflects the principle of proportionality in both psychosocial and digital safety governance—interventions are matched to risk intensity and resource availability, improving feasibility in real school conditions.

Added value and practical implications for SR and PL

The integrated model proposed in Chapter 4 has three main contributions for Slovakia and Poland:

1. It operationalises the triadic SEE concept by explicitly connecting physical, socio-emotional and digital measures within one implementation logic, addressing the contemporary inseparability of educational safety and cybersecurity (Bierecki et al., 2025).
2. It strengthens the governance dimension by embedding safety into leadership, evaluation mechanisms (Safety Index, audits) and implementation fidelity processes, thus moving beyond episodic crisis responses.
3. It offers a capacity-building pathway by specifying where teacher competence development must occur across tiers: universal norm-setting and classroom management, targeted group-based regulation strategies, and indicated crisis intervention and threat assessment routines (Jablonský, 2017;

Konopczyński, 2018; Mazur, 2020).

In line with OECD (2023) reasoning, the discussion supports the conclusion that improved safety is likely to interact positively with learning quality: schools with predictable climates and reliable crisis procedures reduce disruption, increase attendance and protect well-being—conditions that enhance instructional effectiveness.

Limitations and directions for further research

Although the present contribution synthesises empirical findings and proposes a coherent model, the evidence base discussed implies several constraints. First, many cited indicators reflect short-term or event-driven contexts (2024), which limits causal inference about long-term effectiveness. Second, implementation fidelity—identified in Chapter 4 as decisive—requires systematic measurement in Slovak and Polish schools, as variation in adherence can substantially alter outcomes. Third, external socio-economic variables and broader community risk conditions remain influential and should be incorporated into future mixed-methods research designs to avoid over-attributing safety outcomes to school-level interventions alone (Pierzak & Bursová, 2025).

Future studies should therefore focus on longitudinal evaluation of multi-tier implementation, linking Safety Index indicators to well-being and learning outcomes, while also assessing staff cyber preparedness and psychosocial competence as mediating variables (Biernacki et al., 2025; Olejníková et al., 2025).

Conclusion

This study contributes to the contemporary discourse on secondary school safety by advancing a theoretically grounded and practically operational three-tier intervention model that reflects the current risk landscape in Slovakia and Poland. Building on the triadic conceptualisation of a safe educational environment (physical, socio-emotional and digital), the model responds to the empirical and policy reality that school safety has become increasingly shaped by hybrid constellations of threats, including cyber incidents and disinformation, alongside persistent challenges related to violence, disruptive behaviour and psychosocial vulnerability (Biernacki et al., 2025; EDMO, 2024). The proposed framework therefore shifts the focus from fragmented, event-driven measures

toward a systemic, resilience-oriented approach that aligns governance, classroom processes and individual support mechanisms.

The synthesis of evidence presented across chapters supports the conclusion that meaningful safety gains are most likely when schools combine at least two tiers of intervention—universal and targeted—because this pairing stabilises the normative climate, strengthens preventive capacity and reduces escalation pathways before crises reach the indicated level. In this sense, the model frames safety not only as a protective prerequisite for teaching and learning, but also as a quality condition: predictable rules, relational trust and digitally secure routines reduce instructional disruption and create conditions conducive to academic engagement and well-being (Hanuliaková, 2021; Olejníková et al., 2025; OECD, 2023). Importantly, the model highlights that digital safety cannot be treated as an auxiliary topic; rather, it must be integrated into school safety governance through clear responsibility structures, staff competencies and routine monitoring of cyber risks, consistent with the understanding of cybersecurity as a multidimensional organisational process (Bierecki et al., 2025).

Based on the integrated analysis, three implications emerge as central for educational policy and secondary school practice in Slovakia and Poland:

1. Institutionalise safety monitoring and implementation quality control. Schools should implement regular Safety Index audits and embed monitoring of implementation fidelity into leadership routines, ensuring that safety procedures are not only formally adopted but enacted consistently across the school year. This recommendation is reinforced by evidence that organisational planning quality and systematic evaluation mechanisms are associated with stronger safety outcomes and improved educational performance (OECD, 2023; Woynarowska, 2023).

2. Strengthen teacher preparedness as a core safety determinant. The findings underscore that teachers function as frontline agents of safety across socio-emotional and digital domains, yet persistent gaps remain in pre-service and in-service preparation for crisis response, digital incident management and the regulation of disruptive behaviour (Mazur, 2020; Bierecki et al., 2025). Accordingly, teacher education should incorporate mandatory, practice-oriented modules that integrate crisis procedures, legal responsibilities, psychosocial support strategies and cybersecurity awareness.

3. Develop multi-agency partnerships for indicated interventions. While universal and targeted layers produce the greatest preventive leverage, the indicated tier requires coordinated capacity involving school psychologists, specialised counselling services, health providers and, where appropriate,

law-enforcement and cybersecurity actors. Strengthening these partnerships enhances response speed, reduces secondary harm and supports pupils' recovery and reintegration after safety incidents (Šrobárová & Bursová, 2023).

From a research perspective, the proposed model provides a structured basis for rigorous evaluation. Future studies should prioritise longitudinal designs capable of tracking safety, well-being and academic trajectories over multiple years, ideally complemented by quasi-experimental or randomised evaluations of multi-tier implementation. Such research should also examine implementation fidelity as a mediating mechanism and incorporate digital risk indicators, given the growing centrality of cybersecurity and hybrid threats for school functioning (Bierecki et al., 2025).

In conclusion, the evidence and theoretical reasoning presented in this paper support the view that investment in school safety constitutes a strategic lever for sustainable educational development. For Slovakia and Poland, strengthening safe educational environments is not only a matter of risk reduction but an essential condition for protecting mental well-being, maintaining public trust in education and ensuring that secondary schools can fulfil their societal mandate under increasingly complex physical, socio-emotional and digital pressures.

The paper is an output from: KEGA001VŠDTI 4/2025 “*Strategies for Supporting a Safe Environment and Well-being in Education*” and WDSC/USA 09/05/2025 “*Safe Learning and Social Work Environments: Supportive Interventions and Psychological Care.*”

References:

- Bierecki, D., Karpiuk, M., Kelemen, M., Prylipko, S. (2025). The impact of digital transformation on cybersecurity in Poland, Slovakia, and Ukraine. *Prawo i Więź*, 6(59), 474–495. <https://doi.org/10.36128/wppkhn68>
- Bilčík, A. (2018). Podpora záujmu žiakov a ich spokojnosti s vyučovaním na stredných školách. In K. Berková & K. Krpálková Krellová (Eds.), *Schola nova, quo vadis?* (pp. 31–36). Extrasystem.
- Bilčík, A., Balážová, J. (2021). *Na ceste ku kvalite a inklúzii v strednej škole*. Nová Forma.
- Borecka-Biernat, D. (2022). *Bezpieczna szkoła: Uwarunkowania i perspektywy*. Wydawnictwo Uniwersytetu Wrocławskiego.
- Caplan, G. (1964). *Principles of preventive psychiatry*. Basic Books.

- Clarke, K., Jones, P., Williams, L. (2023). *eSafety schools: Integrating cyber-safety into the curriculum*. Australian eSafety Commission.
- Cornell, D. (2023). Effectiveness of behavioural threat-assessment teams in U.S. schools: A meta-analysis. *Journal of School Violence*, 22(1), 1–20. <https://doi.org/10.1080/15388220.2022.2159813>
- Davies, R., Ellis, K., McKay, J. (2023). Targeted Mental Health in Schools 2.0: Outcomes for secondary students. *Educational Psychology in Practice*, 39(2), 145–162. <https://doi.org/10.1080/02667363.2023.2179431>
- Demagog. (2024). *Raport o fałszywych alarmach bombowych w placówkach oświatowych*. Fundacja Demagog.
- EDMO. (2024). *Hybrid threats and disinformation targeting public institutions in Central Europe*. European Digital Media Observatory.
- Emmerová, I. (2024). Bezpečnosť školského prostredia. *Studia Scientifica Facultatis Paedagogicae Universitatis Catholicae Ružomberok*, 23(3), 19–25.
- European Commission. (2023). *Whole-school approach to safety and well-being*. DG EAC.
- Hanuliaková, J. (2021). *Pregraduálna didaktická príprava budúcich učiteľov na prácu s pravidlami v edukačnom prostredí*. Týn nad Vltavou: Nová Forma. 194 s.
- Horner, R. H., Sugai, G. (2023). Positive behavioral interventions and supports: Twenty-five years of research and practice. *Review of Educational Research*, 93(3), 387–417. <https://doi.org/10.3102/00346543231151359>
- Jablonský, T. (2017). Vzdelávanie a školstvo – výzvy, sklamania, očakávania. *Studia Scientifica*, 1, 13–18.
- Konopczyński, M. (2018). *Profilaktyka agresji w szkole*. PWN.
- Mazur, J. (2020). Teacher preparedness and crisis response in Polish schools. In *Relacje rówieśnicze i zdrowie polskiej młodzieży* (pp. 113–129). Instytut Matki i Dziecka.
- Mazur, J., Borecka-Biernat, D., & Woynarowska, B. (2024). Cyberbullying of teachers and its impact on well-being. *Educational Management Administration & Leadership*, 52(4), 601–620. <https://doi.org/10.1177/17411432221116744>
- OECD. (2023). *Education at a glance 2023: OECD indicators*. OECD Publishing. <https://doi.org/10.1787/eag-2023-en>
- Olejníková, A., Porubčanová, D., Bočková, K., & Hanuliaková, J. (2025).

- Positive psychology in Slovak schools: Pathways to well-being. *Journal of Ecohumanism*, 4(1), 2224–2271.
- Pierzak, D., Bursová, J. (2025). The environmental crisis and social work: Interdisciplinary challenges and emerging intervention perspectives. In *Kryzys ekologiczny a praca socjalna – interdyscyplinarne wyzwania* (pp. 129–148). UP Press.
- Pino-James, E. (2022). Fidelity matters: The role of implementation integrity in PBIS outcomes. *Preventing School Failure*, 66(4), 278–287. <https://doi.org/10.1080/1045988X.2022.2054933>
- SAMHSA. (2022). *Whole-school mental health framework*. Substance Abuse and Mental Health Services Administration.
- Šrobárová, S., Bursová, J. (2023). Crisis intervention of helping professionals during armed conflict. *Ad Alta: Journal of Interdisciplinary Research*, 13(1), 252–256.
- Szumski, G. (2022). Participatory decision-making and bullying prevalence: A longitudinal study. *Polish Psychological Bulletin*, 53(3), 187–197. <https://doi.org/10.24425/ppb.2022.141942>
- UNESCO. (2022). *Global status report on school violence and bullying*. UNESCO Publishing.
- UNESCO. (2023). *Media and information literacy for a sustainable future*. UNESCO Publishing.
- Úrad na ochranu osobných údajov. (2024). *Stanovisko k Národnému kamerovému projektu*. ÚOOÚ.
- WHO. (2023). *Guidelines on mental health and psychosocial support in schools*. World Health Organization.
- Woynarowska, B. (2023). Functional school safety: A conceptual model for Central Europe. *Journal of School Health*, 93(2), 134–142. <https://doi.org/10.1111/josh.13254>
- Wysocka, E. (2020). *Kompetencje społeczne młodzieży a klimat szkoły*. University of Silesia Press.
- Zapletal, L. (2023). *Záškoláctví*. Nová Forma.