



Proposal for an Interactive Tool for Assessing Vulnerabilities of Schools as Soft Targets

Samuel Hubočan^{1,*} , Radovan Hubočan¹, Matúš Madleňák¹ ,
Katarína Kampová¹ 

¹ University of Zilina, Faculty of Security Engineering, Department of Security Management
Univerzitná 8215/1, 01026 Zilina
*samuel.hubocan@uniza.sk

Abstract. The paper deals with the design and development of a prototype interactive software tool for assessing the vulnerabilities of the security system of schools as soft targets. The aim of the paper is to present the results of research focused on identifying the absence of a unified technological solution for the systematic analysis of vulnerabilities of school facilities in the conditions of the Slovak Republic and to propose a prototype of such a solution using the Python programming language. The tool named "Bezpečné školské prostredie" (Safe School Environment) is based on the normative framework of technical standards STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016 and consists of a structured questionnaire with 105 questions in five areas of the school security system. Internal verification of the prototype confirmed its functionality and usability while identifying several opportunities for further development, including transformation into a web application and extension with comprehensive risk management.

Keywords: school security, soft targets, vulnerability assessment, software tool.

1 Introduction

The increasing number of violent incidents in school environments (not only in Slovakia) has sparked intense professional discussion in recent years about the need for a systematic and technologically supported approach to the security of educational institutions. Media attention paid to tragic events, such as the knife attack at the school in Vrútky in 2022 or the axe attack at the secondary school in Nováky, points to the fact that schools are vulnerable to violent attacks [1, 2, 3]. For this reason, there is a need for systematic application of security measures that increase the resilience of schools. The current technological progress of the 21st century opens new possibilities for the protection of soft targets and security management, including interactive software solutions. The institutional framework in the field of school security in the Slovak Republic is gradually progressing [4, 5]. However, it is still possible to identify a fundamental gap consisting in the absence of a unified technological solution that would allow analysing the vulnerabilities of the school security system.

2 Theoretical Framework

International professional literature clearly classifies schools school facilities and educational institutions as soft targets. According to several authors, soft targets are events, objects or places where masses of people gather, are accessible to the public and are not sufficiently protected from various, especially violent, threats. Schools, based on their nature, can be characterized as places with a high concentration of people in their premises, relatively unrestricted public access (especially in the morning and afternoon), insufficient access control mechanisms, and the absence of continuous monitoring [6, 7, 8].

Attacks on school facilities are a global phenomenon with serious psychosocial consequences. They include bombings, active shooter attacks, but also other physical and verbal attacks by students on peers or teaching staff [9]. Research by Gerberich et al. [10] conducted in the United States of America demonstrated that there is a higher risk of physical assault among special education teachers and school social workers, with schools located in urban environments being exposed to a higher risk. Hirschfield [11] points out that the risk of victimization on school grounds is higher than outside of it, with educational institutions forming social bonds, peer groups and, in adverse conditions, the emergence of delinquent subcultures.

Professional literature also points out the growing incidence of violent extremism in the school environment. Horgan et al. [12] state that in the case of an active attacker whose actions fulfil a political or religious goal, one can speak of terrorist acts. Amrozy [13] emphasizes that the prevention of shooting attacks should use a combination of physical, technical and organizational security measures supplemented by training simulations. At the same time, the measures introduced must not disrupt the pedagogical process. This conclusion is also supported by Cook et al. [14] and Vel'as et al. [15] according to which security management in schools should not disrupt education and at the same time should build an overall security culture.

2.1 Technical Standards and Solutions

The key normative document related to the area under investigation is the standard STN P CEN/TS 14383-6: 2022 Crime prevention - Spatial planning and design of buildings - Part 6: Schools and educational institutions (referred to as "STN P CEN/TS 14383-6: 2022"). The standard contains recommendations for measures aimed at reducing crime and other anti-social activities against persons and property through preventive risk management. The term vulnerability is defined in the standard as a weakness leading to susceptibility to a threat. This is a condition that, due to the existence of a weakness, allows the threat to cause damage to the asset [16].

The aforementioned standard is also utilized by the Czech technical standard ČSN 73 4400: 2016 Crime prevention – security management in the planning, implementation and use of schools and school facilities, which in its appendix describes the risk assessment process, vulnerability analysis, metrics for expressing the probability and severity of the consequences of risks, as well as metrics for determining the acceptance/non-acceptance of risks [17]. The practical application of this standard in the Czech environment is documented by Sladký and Brečka [18] in the publication Safe

school manual, which emphasizes the regular analysis of vulnerabilities as the core of school security management and risk management. At the same time, it is necessary to mention standards such as ISO 31000 Risk Management - Guidelines and ISO 22341 Security and Resilience - Guidelines for the prevention of crime through environmental design. The mentioned standards represent a framework for the application of security measures, which, due to their nature, are capable of not disrupting the pedagogical process and the character of the school environment.

Within the framework of the analysis of available software solutions, it is possible to identify four main categories of tools used in the school environment. Their application in different countries of the European Union is graphically illustrated in Figure 1.

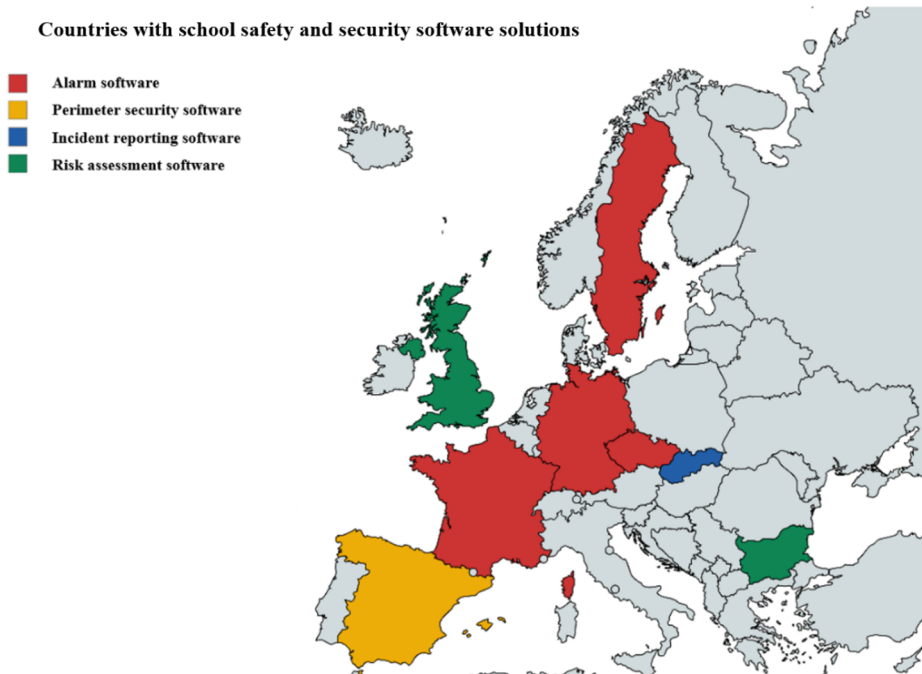


Fig.1 Solutions in different countries (Source: [19-27])

- Alarm software – tools designed to generate alarm messages and coordinate in emergency situations. Examples include the Czech solution Safe School 2.0 [19], the German applications NOKO! [20] and NICA [21], the French software ÉcoleAlerte [22] and the Swedish platform Cosafe [23].

- Perimeter security software – the Spanish solution OnTrack [24] working on the principle of a virtual waiting room and biometric identification when picking up students.

- Incident reporting software – this is a “whistleblowing tool”. In Slovakia, RESQL software is available [25], which allows students to anonymously report bullying and violent behaviour.

- Risk management and assessment software – the British 360 Degree Safe from SWGfL [26] and the Bulgarian academic prototype of a tool for assessing cybersecurity risks in educational institutions [27].

The key finding of the comparative analysis is that these tools are created mainly by the commercial private sector and their use in practice is usually paid and voluntary. The voluntary nature of the software implementation, financial costs and ignorance of their existence lead to significant differences in the level of security in individual schools. It has also been shown that there is no unified technological tool that would systematically analyse the vulnerabilities of a school's security system based on applicable technical standards and be available free of charge.

The comparative analysis of existing software solutions reveals that the proposed tool "Bezpečné školské prostredie" prototype is original in three distinct and cumulative respects, none of which is fulfilled simultaneously by any of the identified commercial or academic tools [19-27]. First, in terms of functional orientation, the majority of available tools (Safe School 2.0, NOKO!, NICA, ÉcoleAlerte, Cosafe) perform a reactive function, generating alarm messages only at the moment a security incident occurs, whereas the proposed prototype performs a proactive, preventive function by systematically identifying and assessing vulnerabilities before an incident takes place. Second, in terms of scope of coverage, the tool that overlaps most closely in content with the proposed prototype is the British platform 360 Degree Safe. However, while 360 Degree Safe is limited exclusively to online security, the proposed prototype addresses the complete physical security system of a school building, comprising the location and position of buildings, the perimeter, the building envelope, the internal space, and organisational measures. Third, in terms of normative grounding and accessibility, unlike the identified commercial solutions, which are typically proprietary and require licensing fees, the proposed prototype is directly derived from the requirements of STN P CEN/TS 14383-6:2022 and ČSN 73 4400:2016 and is made available free of charge, thereby removing both the methodological ambiguity and the financial barrier associated with existing commercial alternatives. This combination of a preventive function, comprehensive physical-security scope, and free normatively anchored design has not been identified in any of the reviewed tools and constitutes the primary contribution to originality of the proposed solution.

3 Methodology

The main objective of the paper is to design and create a prototype of an interactive software tool for assessing vulnerabilities in school security systems. The proposal considers the normative basis of STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016.

In achieving the main objective, the following research questions are discussed:

- Is it possible to design a functional prototype of an interactive software tool model for assessing vulnerabilities in school security systems, which is based on the normative framework of STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016?

- Is the tool verifiable in real deployment conditions and generates structured output usable in the school security management process?

When creating a school vulnerability analysis, the checklist method based on GAP analysis logic was used, where all security recommendations based on the STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016 standards were systematically extracted and transformed into a set of measurable evaluation questions. The logic in creation of the 105 questions based on the normative standards is based on these steps:

- the standard (STN P CEN/TS 14383-6: 2022 or ČSN 73 4400: 2016 states a direct security measure that must be applied in an educational institution.
 - *Example: Clearly marked border against unwarranted entry made up of a fence or other barrier is prerequisite for secure space. (As stated in both normative standards)*
- Using gap analysis logic, the standards state a desired situation. Each normative recommendation was reformulated as a closed, measurable “yes/partial/no-type” statement or question. In a section “Perimeter” within the prototype there is a part dedicated to this specific security measure.
 - *Example:*

Table 1 Example of security measure evaluation

<i>Question 15/105</i>		
<i>Section perimeter – fences and borders</i>		
<i>Variation of choices the user can select (user sees only these choices)</i>	<i>Numerical equivalent</i>	<i>Meaning</i>
<i>A whole school area is clearly separated and marked from public area by a fence or a similar barrier.</i>	<i>1</i>	<i>The security measure is applied in full extent.</i>
<i>A majority of a school area is clearly separated and marked from public area by a fence or similar barrier. There are some parts missing a definite barrier or marking.</i>	<i>2</i>	<i>The security measure is applied partially.</i>
<i>There is no clear separation and marking of school area from a public area by a fence or similar barrier.</i>	<i>3</i>	<i>The security measure is not applied.</i>

- The user selects a choice that describes their particular educational institution the best and goes forward to the next question.

Security recommendations are divided according to the level of school protection into the location and position of buildings, perimeter, envelope, internal space and organizational measures of the school. This classification is in accordance with the classification used in the standards under review. Wording of questions, statements and numerical values used in the prototype were subjected to the discussion with the consortium of experts within national project APVV-23-0437 Strategy and Methodology

for Protecting Soft Targets with a Focus on Elementary, Middle, and High Schools. After the first round of initial testing with participating educational institutions the user choices and numerical values will be discussed with experts and reevaluated.

For the purposes of classifying the overall level of school vulnerability, an expert evaluation method was applied. Relevant quantitative intervals (thresholds) of vulnerabilities are a result of the expert evaluation within the APVV project consortium and may adjusted in the future.

The software development of the tool prototype is guided by the software life cycle model (waterfall model). This model assumes linear sequential phases, such as requirements, design, development, testing, deployment, maintenance [28].

The development of the tool prototype took place from July 2025 to December 2025 in the Visual Studio Code development environment in the Python programming language. The choice of Python was based on its characteristics relevant to the given application domain: syntactic clarity, a rich ecosystem of libraries for graphical interfaces, data processing and document generation, as well as the wide availability of the community to solve technical problems. The basic principles of UX design were applied to the user interface design using the Canva tool.

The verification of the prototype has not yet been conducted in a real educational environment by school staff. Such testing is expected by the end of year 2026 after which there will be a professional discussion with engaged users and consortium of experts within the national project APVV-23-0437.

4 Results

The main part of the prototype consists of 105 structured questions divided into five areas of the school security system, based on the standards STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016. The distribution of questions according to the analysed areas is shown in Table 2.

Table 2 Analysed areas of the school security system

No	Analysed area	Number of questions within a checklist
1.	Location and placement of buildings	14
2.	Perimeter	30
3.	Building envelope	19
4.	Interior of buildings	23
5.	Organizational measures	19
Number of all questions		105

The vulnerabilities (lack of security measures) arising from the standards under investigation may allow a threat (attacker or perpetrator) to cause harm to life, health or property of the school. Individual questions are evaluated by the user in the form of an interactive checklist. Two or three answer options are available for each question, which are assigned numerical values (1, 2, 3). Value 1 represents a state without an

identified vulnerability (ideal state), value 2 a state with partial measures applied, and value 3 a state without any measures taken (existence of untreated vulnerabilities). The tool does not allow skipping any question and allows revision of previous answers. The school database, from which the user selects the analysed school, is based on the official list of 3,864 schools of various types for the 2025/2026 school year, managed by the Centre for Scientific and Technical Information of the Slovak Republic.

A secondary component of the prototype consists of four automated activities: calculating vulnerability values, determining the overall vulnerability of the object (based on an arithmetic average), generating an output report and saving the report to a remote storage.

The vulnerability value of each analysed area is calculated as the arithmetic average of the numerical values of the answers in each area, rounded to two decimal places. The overall vulnerability of the whole school is the arithmetic average of the vulnerability values of all five analysed areas. The interpretation of vulnerabilities is carried out using point intervals, the design of which is inspired by the expert assessment method according to ČSN 73 4400: 2016 and consortium of experts within national project APVV-23-0437. The interpretation of the overall vulnerability is shown in Table 3.

Table 3 Proposal for an assessment of the overall vulnerability of the school

Level of Vulnerability	Threshold	Description
Critical vulnerability	<2,5 – 3,0>	The school must urgently implement new measures for all assessed parts. After their implementation, it is necessary to immediately perform a vulnerability analysis again.
High vulnerability	<1,6 – 2,5)	The school must strengthen the selected assessed parts of the security system, especially those with the highest numerical value of vulnerability. After their implementation, it is necessary to immediately perform a vulnerability analysis again for at least the selected assessed parts.
Medium vulnerability	<1,3 – 1,6)	The school is recommended to take measures within the assessed parts that show the highest vulnerability value. It is necessary to perform a vulnerability analysis at regular intervals and monitor the implemented security measures.
Low vulnerability	<1,0 – 1,3)	It is necessary to perform a vulnerability analysis at regular intervals and monitor the implemented security measures.

The thresholds and intervals can be subjected to corrections in the future, after first round of testing on participating educational institutions.

The results of the vulnerability analysis are visualized for the user in the form of a bar chart generated using the matplotlib library, in which the columns are color-coded according to the achieved vulnerability level, as shown in Figure 2.

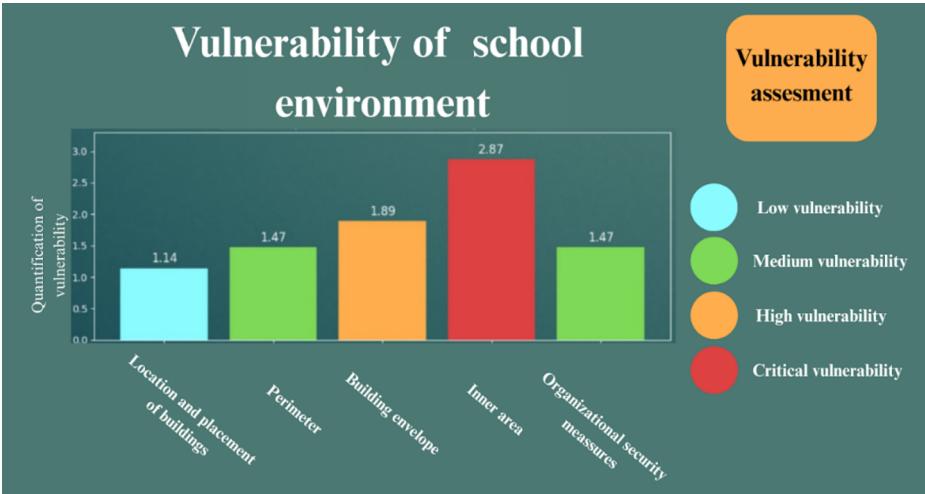


Fig. 2 Graphical representation of results

The user can then generate and download the output report of the analysis. The report is saved not only to local storage, but also automatically to the remote cloud storage Dropbox, where the reports are named with a combination of the school code and the string outputreport.pdf. The current prototype does not yet implement a comprehensive data protection and cybersecurity framework. The automatic storage of generated reports on the remote cloud service Dropbox is presented in this study primarily as a proof-of-concept functionality, demonstrating the technical feasibility of centralised report storage for potential future use by public administration bodies (e.g., the Crime Prevention Office) in support of national monitoring of school vulnerability levels. At the current stage of development, aspects such as access control, encryption of data in transit and at rest, formal risk assessment of the third-party cloud integration, and full compliance with the General Data Protection Regulation (GDPR) have not yet been systematically addressed and represent an acknowledged limitation of the prototype. Since the generated reports contain a school identification code, any future deployment beyond the prototype stage will require a dedicated data protection impact assessment, the implementation of role-based access control and encrypted storage, and the definition of a clear legal basis and data retention policy in accordance with GDPR requirements. Addressing these cybersecurity and data protection requirements, together with an evaluation of alternative storage solutions compliant with EU data residency principles, is therefore identified as an essential prerequisite for transforming the current

prototype into a production ready tool and is included among the priority directions for future development of the "Bezpečné školské prostredie" tool.

Measuring the load on the computer's system components during a standard scenario of using the tool's prototype yielded the following results:

Table 4 System Requirements

Measured parameter	Value
Maximum RAM usage	8.8 megabytes
CPU usage	1 processor core loaded at 78%
Storage usage	63.1 megabytes (without generated output reports)

The measurement results indicate that the tool has low requirements for computer hardware components, which is a significant advantage in terms of its deployment in a school environment with heterogeneous hardware equipment.

Verification of the tool prototype on several random workstations with the Windows operating system confirmed its functionality and usability in practice. During the verification, five categories of frequent errors were identified:

1. Incorrect display of graphical interface elements due to different resolution settings and system settings.
2. Cutting off school names in the drop-down list.
3. Failure to display the generated graph at the vulnerability assessment stage.
4. Failure to remove the binding to the Return key, which caused undesirable program behaviour.
5. Failure to display letters of the Slovak alphabet in the generated report.

5 Discussion and Conclusion

Based on the presented results, it can be stated that the main objective was achieved and the answer to the research question is positive, with the following justifications:

- The established normative basis and requirements of the standards were considered and successfully implemented. Criteria extracted from the STN P CEN/TS 14383-6: 2022 and ČSN 73 4400: 2016 standards (105 questions in 5 areas) were used in the vulnerability analysis in the form of a checklist based on the logic of GAP analysis, thus ensuring the content validity of the evaluation framework.

- The tool was successfully created in a Python environment with low system requirements (max. 8.8 MB RAM, 63.1 MB disk space), which confirms its technical feasibility and usability on school hardware.

- Verification on multiple workstations confirmed the basic functionality. Of the five identified error categories, three were removed; the remaining two (displaying the interface at different resolutions, cropping school names) had no impact on the correctness of the calculations or the generated analytical output.

- An automatically generated PDF report containing school identification, vulnerability analysis according to five areas, visualization of results, and overall interpretation

of the vulnerability level represents a structured and usable document for school security management.

The proposed prototype of the "Bezpečné školské prostredie" tool differs in its essence from existing commercial solutions. As mentioned, the majority of available tools (Safe School 2.0, NOKO!, NICA, ÉcoleAlerte, Cosafe) focus on a reactive function - i.e. generating alarm messages at the time of a security incident. The "Bezpečné školské prostredie" prototype fulfils a proactive preventive and monitoring function, consisting in the systematic and periodic identification and assessment of security vulnerabilities before a security incident occurs. Of the identified tools, the proposed prototype overlaps most in content with the British platform 360 Degree Safe, but with a key difference - while 360 Degree Safe focuses exclusively on the area of online security, the proposed tool covers the complex physical security system of a school building, including the location, perimeter, building envelope, internal space and organizational measures. In contrast to commercial solutions, the prototype under development represents a free, normatively anchored solution available without additional licensing costs, which removes the financial barrier found with commercial alternatives.

The primary benefit of the tool is to enable internal self-assessment of the school's vulnerability level without the need for external assistance and without additional financial costs. By repeatedly using the tool at regular intervals, it is possible to monitor the trend of vulnerability levels over time and verify whether the measures taken have led to a reduction in vulnerability in specific areas of the security system. The generated PDF report can serve as a basis for school management, founders or other interested parties when planning preventive measures, creating projects aimed at increasing security, or as a supporting argument when defending investments in security.

Based on the information provided, it can be stated that the research questions have been answered. The designed prototype meets all predefined requirements that were part of the research questions, while the identified technical limitations do not represent a fundamental barrier to its practical use, but are a natural part of the research and development cycle at the prototype stage. The main goal can be considered fulfilled.

Internal verification of the prototype on several workstations generally confirmed its technical functionality, while identifying several limitations related mainly to the graphical interface. The verification conducted in this study was limited to technical functionality testing on multiple workstations; systematic usability testing involving representative end-users, such as school principals or security coordinators has not yet been conducted and is identified as a priority direction for future research. The following (apart from real time testing in educational institutions) can be considered as promising directions for further development:

- transformation into a web application – for the purpose of unified graphic design and elimination of functionality dependence on a specific operating system,
- implementation of a GDPR compliant data protection and cybersecurity framework, including access control, encryption, a formal data protection impact assessment, and a defined data retention policy, prior to any deployment beyond the prototype stage,

- expansion to include comprehensive risk management – practical application of processes within the framework of ISO 31000 and ČSN 73 4400: 2016 would transform the tool into a comprehensive risk management system,
- internationalization – translation of text elements into foreign languages would enable the tool to be used in foreign schools,
- aggregated report analysis – centralized storage and analysis of output reports would enable mapping of schools according to the level of vulnerability at the national level, thus creating a tool for targeted support of the most vulnerable group of schools.

The proposed prototype of the tool opens further research questions regarding verification of the functionality and acceptance of the tool in specific schools, assessment of the effectiveness of the outputs in targeted support of vulnerable schools, as well as the potential for integration with existing school security processes and documentation.

Acknowledgments. This contribution was created with the support of project KEGA 058ŽU-4/2025 Gamification and innovation of teaching aids in the field of criminology and public administration and APVV-23-0437 Strategy and Methodology for Protecting Soft Targets with a Focus on Elementary, Middle, and High Schools.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. VRAŽDA, D. 2020. In an attack at an elementary school in Vrútky, the deputy principal died and the attacker also injured children. He was shot dead by police. *DenníkN, News report*. Available at: <https://dennikn.sk/1927282/utok-na-zakladnej-skole-vo-vrutkach/>
2. MARIŠ, L. et al. 2025. Strategy and methodology for the protection of soft targets in primary, secondary, and higher education institutions. *Proceedings of the INTED2025*; Vol. 1. ISSN 2340-1079 doi: 10.21125/inted.2025.0831
3. THEIMANN, M. 2016. School as a Space of Socialization and Prevention. *Eur. J. Criminol.*, 13, doi:10.1177/1477370815597254
4. Ministry of the Interior of the Slovak Republic, 2026. Handbook for developing a security plan. Available at: <https://www.minv.sk/?makke-ciele-ochrana-narodny-projekt>
5. Ministry of the Interior of the Slovak Republic, et al. 2025. Protection of Soft Targets in the School Environment: Security Recommendations. Available at: <https://www.minv.sk/?makke-ciele-ochrana-narodny-projekt>
6. ZEMAN, T. et al. 2023. Assessing the risk of a terrorist attack against a soft target: the use of expert opinion in threat assessment. *Ad alta-journal of interdisciplinary research*, vol. 13, is. 2, s. 295-298. ISSN:1804-7890
7. KALVACH, Z. 2025. Soft Target Threat Assessment. Available at: <https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>
8. BOROŠ, M. et al. 2018. Development of security at the local level through practical students training. *Proceedings of the INTED2018*; Vol. 1. ISSN: 2340-1079 doi: 10.21125/inted.2018.1136
9. LONGOBARDI, C. et al. 2019. Student-Teacher Relationships and School Safety. *Frontiers in Psychology*. doi: 10.3389/fpsyg.2019.00958.

10. GERBERICH, G. et al. 2014. Case-control study of student-perpetrated physical violence against educators. *Annals of Epidemiology*. doi: 10.1016/j.annepidem.2014.02.006.
11. HIRSCHFELD, P. 2018. Schools and Crime. *Annual Review of Criminology*. doi: 10.1146/annurev-criminol-032317-092358.
12. HORGAN, J. et al. 2024. Understanding and preventing violent extremism in school settings. *Journal of School Psychology*. doi: 10.1016/j.jsp.2024.101346.
13. AMROZY, K. 2024. Securing educational institutions against an active killer on the example of the United States of America. Best practices and recommendations. *Terrorism – Studies, Analyses, Prevention*. doi: 10.4467/27204383TER.24.029.20249.
14. COOK, PHILIP J. et al. 2009. School Crime Control and Prevention. DOI <http://dx.doi.org/10.2139/ssrn.1368292>
15. VELAS, A. et al. 2022. Research of Security and Safety Culture within an Organization. The Case Study within the Slovak Republic. *Security Journal*. doi:10.1057/s41284-021-00291-5.
16. STN P CEN/TS 14383-6: 2022 Crime prevention - Spatial planning and design of buildings - Part 6: Schools and educational institutions
17. ČSN 73 4400: 2016 Crime prevention – security management in the planning, implementation and use of schools and school facilities
18. SLADKÝ, L. et al. 2022. Manuál bezpečné školy: Bezpečná škola a školské zariadenie v kontextu ČSN 73 4400. 1. vyd. Karlovy Vary: Asociace bezpečná škola z. s., ISBN 978-80-908515-2-8
19. Bezpečná škola 2.0 - Komplexní systém pro ochranu škol. 2026. Available at: <https://www.bezpecnaskola.cz/>
20. PAJA Software UG (haftungsbeschränkt). *NOKO – Notfall- & Amokalarm-App für Schulen*. NOKO Notfallkommunikation. Available at: <https://www.noko-app.de/>
21. KRAMER, D. et al. 2026. NICA Software. Available at: <https://nica-software.de/>
22. MAMELLI, A. 2026. École Alerte Available at: <https://ecolealerte.fr/>
23. COSAFE TECHNOLOGY AB. 2026. Skolsäkerhet. Available at: <https://co-safe.com/sv/skolsakerhet/>
24. ONTRACK 2025. Seguridad escolar: salida del colegio. Available at: <https://on-track.global/seguridad-escolar-salida-del-colegio/>
25. RESQL. 2026. RESQL. Available at: <https://resql.raabe.sk/>
26. SWGfL. 2026. 360 degree safe. Available at: <https://swgfl.org.uk/services/360-degree-safe/>
27. GEORGIEV, G. 2025. Cybersecurity And Cyberethics In Bulgarian Schools. *Education & Technology Journal*. Available at: https://www.edutechjournal.org/wp-content/uploads/2025/09/2_2025_346-352.pdf
28. ATLISSIAN. 2026. Waterfall Methodology: A Comprehensive Guide. Available at: <https://www.atlassian.com/agile/project-management/waterfall-methodology>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

