KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 16, No. 1 (2026), p. 24 – 33

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)



Armed attacker as the biggest risk for soft targets (schools)

Ozbrojený útočník ako najväčšie riziko pre mäkké ciele (školy)

Ladislav HÉŽEL[1]

[1]*University of Security Management in Košice*

The manuscript was received on 29.06.2026 and was accepted after revision for publication on 30.06.2026

Abstract:

This article deals with the issue of protecting soft targets with a specific focus on educational institutions in the context of current security threats in the Slovak Republic. The article defines the basic conceptual apparatus, including the differences between soft and hard targets, defines the phenomenon of an armed attacker, an active shooter and a state of amok. It implements a typology of soft targets according to stability and the local security environment, identifies key sources of threats, methods of attack and proposes a comprehensive school protection framework combining technical, regime, organizational and educational measures with the aim of minimizing the vulnerability of these high-risk objects.

Keywords: *soft targets, armed attacker, active shooter, ammo, high profile incident*

Abstrakt:

Tento článok sa zaoberá problematikou ochrany mäkkých cieľov so špecifickým zameraním na školské inštitúcie v kontexte súčasných bezpečnostných hrozieb v Slovenskej republike. Článok vymedzuje základný pojmový aparát vrátane rozdielov medzi mäkkými a tvrdými cieľmi, definuje fenomén ozbrojeného útočníka, aktívneho strelca a stavu amoku. Implementuje typológiu mäkkých cieľov podľa stálosti a lokálneho bezpečnostného prostredia, identifikuje kľúčové zdroje hrozieb, spôsoby útoku a navrhuje komplexný rámec ochrany škôl kombinujúci technické, režimové, organizačné a edukačné opatrenia s cieľom minimalizovať zraniteľnosť týchto vysoko rizikových objektov.

Kľúčové slová: *mäkké ciele, ozbrojený útočník, aktívny strelec, amok, vysoko profilový incident*

This work is licensed under a Creative Commons Attribution 4.0 International License.

Introduction

In the sphere of modern security management and population protection, a fundamental paradigm shift has occurred in recent decades. While classical security theory primarily envisioned protection systems for critical infrastructure, military facilities, and state institutions, the current asymmetric nature of security threats shifts attention to places with high concentrations of civilian populations. These objects and spaces are defined within professional literature as "soft targets". In circumstances of the Slovak Republic and the Central European region, schools and school facilities come to the forefront as the most vulnerable and at the same time the most socially sensitive soft targets. School has historically been perceived as a protective place, a safe environment protected from external conflicts. However, global incidents, as well as recent events in the Central European region, clearly prove that schools are becoming the primary target of attacks with the aim of maximizing victims. An attack by an armed assailant, often classified as an active shooter attack, represents an extreme crisis situation to which normal security and pedagogical procedures cannot respond without prior systematic preparation.

The objective of this article is to analyze the structure of threats to soft targets, specify the position of schools within their typology, and to propose an integrated protection system that minimizes the risk and consequences of a potential attack, based on theoretical principles, legislative standards of the Slovak Republic and current scientific knowledge (e.g. Apeltauer, 2019; Dvořák, Šimonová, Veľas, 2024).

1 Definition of basic terms

A soft target is a place with a high concentration of people and minimal security against violent attacks, or an environment that is easily accessible, attracts large numbers of people, and is an easy target for attack using available weapons and relatively simple tactics. For example these are, schools and school facilities, church buildings, hospitals and health care providers, cultural centers/events, sports centers/events, night clubs, theaters, opera houses, cinemas, cafes, restaurants, public passenger transport facilities and vehicles. [6]

An active shooter is a dangerous offender who has chosen to use a weapon against other people to achieve his goals. It is usually about individuals, but it can also be about a group of perpetrators. They have no inhibitions about any action aimed at killing or injuring as many people as possible.

A rampage is a sudden mass attack on people or objects, usually led by an individual in a violent, furious, wild, or uncontrollable manner. This criminal entitlement indicates a short-term action of an active shooter.

A high-profile incident is a crisis situation consisting of an actual or threatened illegal situation caused by a person or a group of people, in which one or more people have been killed or there is a real threat of killing more than one person. These actions may cause serious health injury, health disorders, damage on a large scale, or causing other serious consequences, e.g. killing or injuring people, taking a hostage, restricting personal freedom, kidnapping, extortion, use of explosive devices, biological substances, chemical substances or nuclear material, regardless of later legal qualification. [6]

2 Attractiveness of soft targets

As stated by Dvořák, Šimonová and Veľas (2024), the main defining feature of a soft target is its accessibility and high population density. There is an axiom in security saying: A soft target means an easy target.

The attractiveness of these objects for attackers lies mainly in minimal protection and a high volume of people in one place. For the perpetrator, the following attractiveness criteria play a key role: easy and unnoticed access, guaranteed media attention, significance of objective, or high symbolic value (Dvořák, Šimonová, Veľas, 2024, p. 45). An attack on children in schools affects the most sensitive areas of the social psyche and causes mass panic. [1]

3 Identification of soft targets and the local security environment

In order to be able to propose effective security measures, it is necessary to carry out a thorough identification of soft targets. To identify soft targets that could represent a potential object of attack by terrorists or individuals or organized groups, it is most important to focus on objects in a specific local environment. [3]

The local security environment consists of a set of materialistic, economic, social, political and spiritual factors that largely influence the existence, formation and activity of reference objects.

Within a specific local environment, based on the criterion of time stability, we can identify three basic types of objects/soft targets [2]

- **permanent objects**: to which public access is practically unlimited, for example: railway, bus stations, etc.;
- **temporary objects**: to which public access is limited at certain times of the day (opening/operating hours), for example schools, shopping centers, offices, cinemas, etc.;
- **occasional objects**: where the long-term access period for the public is not predetermined and people gather here only occasionally, for example markets, fairs, places of pilgrimage, etc.

According to the author Apeltauer (2019), the ideal criterion is permanence, according to which he subsequently divides them into permanent and temporary. A more detailed breakdown of permanent and permanent soft targets is shown in the following diagram (Fig. 1).

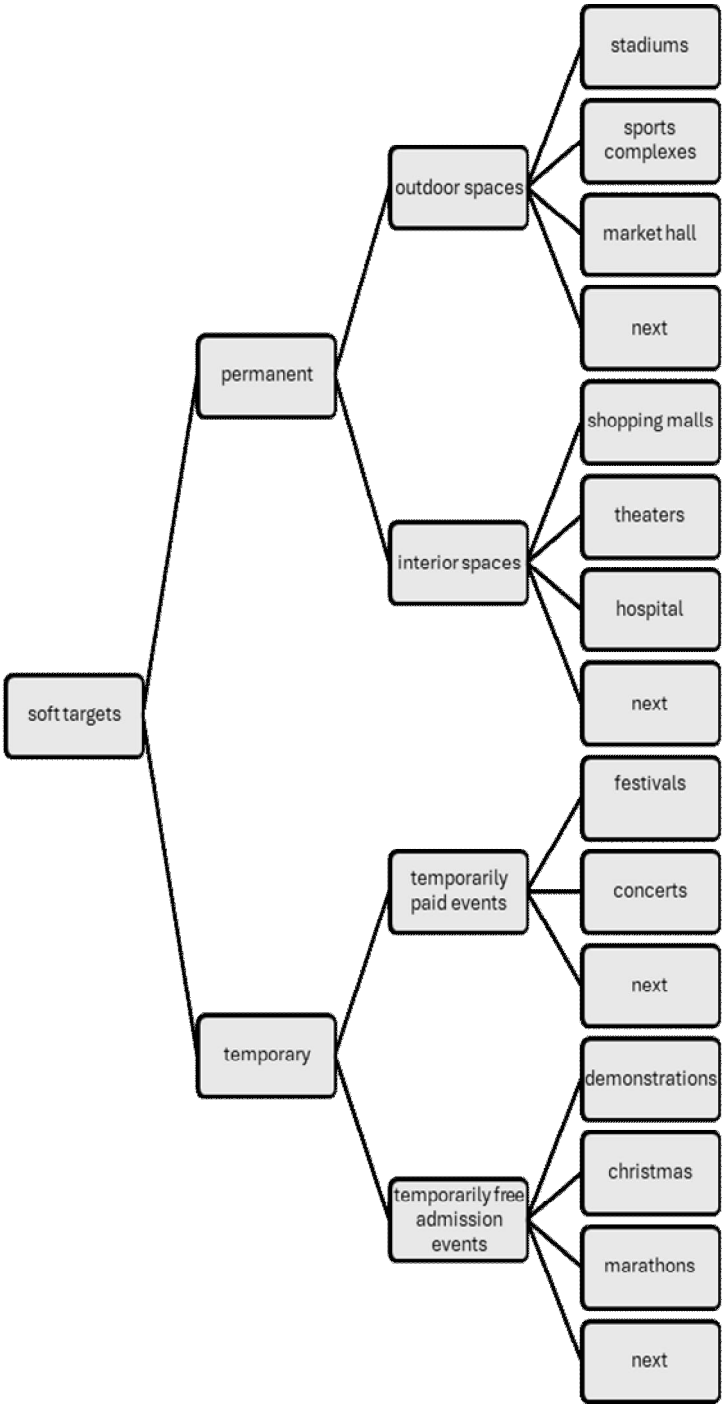


fig. 1 Distribution of soft targets [2]

4 Threat sources for soft targets

Correct identification of threat sources (people and their groups or organizations that are potential attackers) is essential for their evaluation. We can protect e.g. people, property, information and reputation. As for protecting soft targets, we focus on protecting people from violent attacks, respectively for their lives and health.

Possible sources of threats to soft targets in the Slovak Republic (i.e. individuals and groups):

- **Violators involved in classic criminal activity**: perpetrators motivated by material gain (robberies) whose attack escalates into massive violence due to the failure of their original plan or the resistance of the victims.
- **Mentally ill people**: individuals suffering from serious mental disorders (schizophrenia, severe psychoses, delusions) in whom rational motivation is absent. Their attack is often unpredictable, sudden and shows signs of amok.
- **Retaliating employees, clients, students, etc.:** this is an extremely dangerous category of the so-called "Insider Threat". They are frustrated people who have experienced real or imagined wrongdoing (dismissal from work, failure to give credit, bullying by classmates). These perpetrators have a huge tactical advantage - they know perfectly the environment of the target, its poorly secured places, the timetable and the response capabilities of the personnel.
- **Organized crime groups**: their attacks on soft targets are more rare, usually related to a show of force, settling scores in the criminal environment or intimidation (eg nightclub attacks).
- **Extremists and people attacking out of hatred (attackers committing so-called hate crimes):** radicalized individuals or groups motivated by racial, national, religious or other intolerance (e.g. attacks on the LGBTI community, attacks on religious objects). Their goal is the elimination of a specific group population.
- **Terrorists**: ideologically, politically or religiously motivated actors whose aim is to systematically spread fear, destabilize state power and force political change through the mass killing of civilians.

Common crime, attacks by mentally ill people and attacks out of personal revenge cannot be ruled out in any setting. [7]

When protecting soft targets, we only deal with the area of personal protection, namely protection against serious violent and terrorist attacks. To assess whether a given soft target can also be a target of organized crime, hate attacks or a terrorist attack, it is necessary to assess the external and internal context of the target.

It is mainly about its symbolism, the people who move in it, the subject of the activity and the environment or the incidents within. In this context, it is appropriate to emphasize that terrorist attacks must be considered especially with regards to the location in which the soft target is located. For example, if a small restaurant is located on a main tourist promenade, it can be hit just like a large sports stadium.

It is recommended to analyze the mentioned sources of threat, which are relevant for the given soft target, and try to achieve the most accurate determination of the specific group or specific individuals who can attack the given soft target. It is acceptable to use "Open Source Intelligence" (OSINT) for this activity. That is, obtaining the necessary security information about people and groups from open sources, including e.g. social networks. Even if the soft target does not have the capability and means to carry out this activity systematically and long-term, it is highly desirable that people responsible for the development of security specify the sources of threats (individuals and groups of people) based on previous knowledge and experience. [7]

5 Attack methods for individual sources of threats

Any specific methods of carrying out attacks differ both between individuals or groups of people (threat sources) given their timeline. Not only will the method of carrying out an attack by terrorist organizations differ from organized crime, but also the method of attacking one terrorist group from another and to individual racist groups attacking each other. Moreover, the whole situation changes over time. Therefore, it is not possible to define a general list of threat methods that would be valid for all soft targets, often not even for individual categories (e.g. a universal list for hospitals, schools, etc.). If such lists appear somewhere, they only have an indicative use, it is better to always reassess them in relation to a specific soft target (at a given time and place).

The source of the basic set of methods of carrying out attacks, which are relevant for all soft targets, is mostly violent activity associated with classic crime, violent attacks by mentally ill people and attacks by workers, clients or students, etc. (basic list):

- assault with a cold weapon (stabbing, slashing, blunt, etc.);
- assault with a firearm (short, long);
- arson attack;
- hostage and barricade situation;
- attacking a soft target by a crowd (violent assemblies);
- explosive in mail;
- poisonous substance in mail;
- planting an imitation explosive;
- placement of an explosive in a certain area (without the presence of an attacker, e.g. stored luggage); false notification of the location of an explosive (or other dangerous substances).

The above guide list of threats represent a starting set of attacks that must be taken into account. They are thus an aid for thinking about what kind of violence can threaten a specific soft target. They are not and cannot be an exhaustive overview of attack methods or an immutable list of what is certain to threaten a particular soft target. At the same time, we emphasize the necessity to consider other ways of carrying out attacks individually for each analyzed soft target. [7]

6 Active shooter

An active shooter is defined as an individual or a group that actively participates in murders or attempted murders in places with a high concentration and to the greatest extent possible. We collectively refer to such a space as a soft target. These are schools, shopping centers, concert halls, squares, etc. This type of violent attack usually involves the use of firearms and can take place in closed or open spaces.

Among the characteristic features of the behavior of active shooters is the search for as many potential victims as possible. The shooter moves quickly and often there is no specific pattern or selection of his targets. The motivation for these actions can be associated with factors such as a mental disorder, hatred towards a certain group of people, or a change in behavior after a significant life event.

An active shooter usually does not intend to create a situation in which he holds civilians hostage and thus cause further intervention for the security forces. However, there are also cases that happened in such a way. From the point of view of legal qualification, these were rather terrorist acts that showed similar characteristics. After completing an attack, the shooter in most cases does not want to be directly confronted by the intervention of repressive security forces and commits suicide. [4]

Schools and school facilities are classified as typical soft targets in security management terminology. They are characterized by a high concentration of people, a low level of ballistic and physical protection and a high degree of public accessibility. Although historically these attributes have been seen as the pillars of an open civil society, they represent a critical vulnerability in the current security environment. The active shooter / active assailant phenomenon has become a priority asymmetric threat that requires a systemic change in the approach to protection of staff and students.

Threat analysis and specifics of the school environment

The risk of an armed criminal attacking a school is specifically due to its unpredictability and extreme dynamics. According to international security analyzes (e.g. studies by the American FBI or CIA):

- **The decisive time factor:** the average incident **lasts 10 to 15 minutes**. The greatest number of loss of life occurs in the **first 3 to 5 minutes**, which usually precedes the arrival of the first officers of the police force.
- **Architectural limits: up to 57% of** school principals state in surveys that the age and layout of buildings (number of glazed areas, corridor

systems without escape zones) directly negatively affect the possibility of implementing effective technical safety measures.

Perpetrator Profile "Insider Threat"

It is crucial for the security manager to understand that school attacks are dominated by the so-called insider threat (internal threat). Slovak and foreign security analysts point to a serious statistical fact: 4 out of 5 attackers (approximately 80%) in the school environment are directly connected to the target institution - they are current or former students, or employees.

This factor radically changes the approach to protection: the attacker perfectly knows the object's topography, daily schedule, escape routes, and weaknesses in the access control system. The motivation is most often personal frustration, long-term bullying, psychological decompensation or radicalization.

7 Design of an integrated school protection system

Based on defining the Action Plan for the protection of soft targets for 2025 and the needs of practice, it is essential that schools implement the so-called concept of multi-level security (Defense-in-Depth). No single measure (e.g. the camera system itself) can stop an active shooter. The measures must be divided into three interconnected pillars. [6]

A. Technical and regime measures (Hard Security)

The aim of these measures is to make it more difficult for the attacker to enter the building, or to slow down his progress throughout the building, which will give the police the time needed to eliminate him.

- **Entrance management and mechanical barriers:** Strict reduction of available entrances to the building should be limited to one main point entry for the public. Other escape exits must be equipped with panic features, which allow escape to the outside easily, while blocking entrance to inside. Implementation of electronic access systems (chip cards for students and staff) and video doormen for the control of external visitors.
- **Internal zoning and "Classroom Lock":** Equipping the doors of all classrooms, cabinets and lecture halls with locks and enabling the function of quick locking from the inside without the need for a key (panic locks). If an attacker enters the corridor, teachers must be able to immediately transform the classrooms into a safe zone.
- **Early warning system and addressable radio**: Installation of acoustic and visual signaling elements, which are different from the fire alarm. An acoustical announcement (eg a code word or a clear command: "Security incident - lock down classrooms immediately") is

key. In the event of a fire, people evacuate to the corridors; in the case of an active shooter, evacuation to the corridors without locating the perpetrator is a fatal mistake.

B. Organizational and educational measures (Soft security)

Technologies will fail if a human does not know how to respond to them. This pillar focuses on people's preparedness.

- **Implementation of the Run-Hide-Fight tactic (Escape-Hide-Fight):** Every school employee must have automated three basic patterns of behavior depending on the location of the attacker:
  1. *Run*: if it is safe and the attacker is in another part of the building, leave premises immediately.
  2. *Hide*: if escape is not possible, lock yourself in the classroom, block the door with heavy furniture, turn off the lights, silence cell phones, and hide out of visual range from the door window.
  3. *Fight:* as an absolute last resort in the event of a direct threat to life - to attack the attacker in a coordinated manner using improvised weapons (chairs, fire extinguishers, books) with the aim of paralyzing him. [5]
- **Regular simulation exercises**: theoretical lectures are ineffective. Schools must, in cooperation with the Slovak Police Force, organize practical exercises in crisis scenarios for staff in order to eliminate panic shock in a real situation.

C. Psychosocial prevention and detection of clues

Prevention is the cheapest and most effective form of protection. As mentioned in the characterization of threats, vengeful students almost always show warning signs before an attack – it is a leakage phenomenon, when the perpetrator confides his intention on social networks, in essays or directly to classmates.

Schools must build multidisciplinary teams (school psychologist, educational counselor, school management) that can detect signs of extreme frustration, cyberbullying, radicalization or mental disorders in students and initiate timely psychosocial or psychiatric intervention before the situation escalates into a state of amok.

Conclusion

An armed attacker in the form of an active shooter represents a threat of the highest degree to schools in the Slovak Republic with potentially catastrophic consequences. Since absolute security in the context of soft targets is an illusion, the primary goal of academic research and security practice must be to systematically

reduce the vulnerability of objects and increase the preparedness of their occupants. The safety of our children cannot depend on improvisation, but must be the result of exact safety planning. Investments in security must not be seen as a one-time cost, but as a permanent process of auditing, creation of standardized methodologies and procedures, technical evaluation of school buildings from the point of view of anti-terrorist protection, training of crisis plans and staff education. Only a prepared soft target can transform itself in a moment of crisis into an environment that can repel an attack or significantly mitigate its fatal consequences.

References

Books:

[1] DVOŘAK, Z., ŠIMONOVÁ, J., VEĽAS, A., Minimum Standard for the Security and Safety Audit of a Higher Education Institution, Ministry of Interior of the Slovak Republic, 2024,

[2] APELTAUER, T., et. al., Ochrana měkkých cílu , Praha Leges, 2019. ISBN 978-80-7502-427-5 , p. 80-85

[3] KUBÍKOVÁ, Z., Identifikácia a hodnotenie mäkkých cieľov v lokálnom prostredí, medzinárodný workshop, Bezpečnosť v lokálnom prostredí 2017, fakulta bezpečnostného inžinierstva UNIZA, Žilina,

[4] DOSS, Kevin a SHEPHERD, Charles. Active Shooter: Preparing for and Responding to a Growing Threat. Reprint. Butterworth-Heinemann, 2015. ISBN 978-0-128-02783-7.

Journals:

[5] Ministerstvo vnútra Slovenskej republiky, 2026. Leaflet Run-Hide-Fight, [online] [cit 10-6-2026] avaible from: https://www.minv.sk/?zakladne-materialy

[6] Ministerstvo vnútra Slovenskej republiky, 2026. ACTION PLAN FOR THE PROTECTION OF SOFT TARGETS FOR THE YEAR 2025, [online] [cit 10-6-2026] avaible from: https://www.minv.sk/?zakladne-materialy

[7] Ministerstvo vnitra České republiky, 2026. Soft Target Vulnerability Assessment, [online] [cit 09-6-2026] avaible from: https://mv.gov.cz/chh/default.aspx

Author:

[1]**col. Ing. Ladislav Hežel, DBA, LL.M** – full-time doctoral student, University of Security Management in Košice, Košťova 1, 040 01 Košice, Slovak republic**,** e-mail:ladislav.hezel@vsbm.sk