

Soft Target Threat Assessment

or what, when, where and from whom
you are threatened

April 2025



2nd revised edition

Compiled by:

Ing. Zdeněk Kalvach

Editing and publishing:

Security Policy Department
Ministry of the Interior, Czech Republic

Contacts:

obp@mv.gov.cz

Police hotline for soft targets:

800 255 255

Web MV:

<https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>

Social media:




-  <https://x.com/vnitro>
-  https://www.facebook.com/vnitro_cz
-  <https://www.youtube.com/user/MinisterstvoVnitraCR>

Table of Contents

Introduction	4
Summary of the soft target threat (degree) assessment procedure	5
Stage 1	5
Stage 2	5
Stage 3	5
Sources of threats to soft targets	7
Methods of attack for individual sources of threats	8
Creating a list of possible methods of attack on a specific soft target	9
Attack localization variations.....	9
Variations of attack timing	10
Soft target threat (degree) assessment	10
Determining the probability of a given method of attack	11
Availability of means of attack	12
The occurrence of the method of attack	12
The complexity of a given method of attack	13
Impact assessment.....	15
Impact on lives and health	15
Impact on a facility	15
Financial impact	16
Impact on the functioning of the affected community.....	16
Assessment of the overall threat level.....	17

Introduction

The purpose of this document is to strengthen the resilience of soft targets in the Czech Republic by employing a systematic approach to their security. The term soft targets is used when describing sites, premises, or events characterized by a high concentration of people and, concurrently, by the absence or a low degree of security against major violent and terrorist attacks.¹

The authors assume, among other things, that the biggest reserve in building soft target security systems is not the lack of resources or material equipment, but their inefficient spending and inadequate knowledge of real needs.

Moreover, it is precisely the effective threat assessment that represents one of the pillars of any high-quality security system because it can detect real threats and their specific form.

This document is a follow-up to the methodology entitled [Basics of Soft Targets Protection](#) published by the Ministry of the Interior in 2016. It includes a theoretical introductory part, which describes the steps necessary to establish functional security measures. One of these steps is to assess the resilience which this document is devoted to. The method of assessment of the protected site is based on the Israeli security school, and it is commonly used by the international security community in securing extremely endangered sites.

This methodology is intended primarily for managers and operators of soft targets, who decide on the development of the se-

curity system of a specific soft target. By this, we mean not only security professionals but also senior management that hires security services, evaluates suppliers' offers and needs to know what to demand and where to direct the security. The role of soft target operators is, therefore, essential.

Given the above, it is necessary to highlight right at the outset that the objective of the threat assessment is not a complicatedly calculated numerical table based on statistical formulas. On the contrary, it is a simple but very purposeful **thought process** that will lead the user in a systematic and proven manner to a better understanding of the risks at hand. **Moreover, it is this knowledge and clarification of the key issues in the process of table processing (not the table itself) that is the purpose of the submitted assessment.**

As is evident from the general methodology entitled [Basics of Soft Targets Protection](#), three consecutive questions must be answered before the elaboration of a threat assessment:

- **What do we want to protect** – identification of the so-called assets (values). These are most often life and health, property, information, but also the reputation of the organization or essential relationships. In the case of soft targets protection, we focus on the protection of human lives and health.
- **Against whom we want to protect our values** – identification of sources of threats (persons, groups of persons). In this section, it is necessary to consider what individuals or groups represent the danger: who would want to hurt me? Such sources of threats may be ordinary criminals, ideologically

oriented hate groups, upset personnel, mentally ill persons, and others.

- **How do these individual threat sources attack? What is the threat from them?** If we know our „enemies“, we need to understand their behaviour. So, we have to ask ourselves: what motivates them to attack, when and where they usually attack, what weapons they attack with, how do they use them?

By clarifying these three questions, a list of specific possible methods of attack that might threaten a specific soft target can then be drawn up. **This list is at the heart of the soft target security system.** The effective setting of the security policy, strategy and all sub-measures are based on this list. It is, therefore, crucial that it is always developed based on careful consideration; it should not be taken over from elsewhere, or it should not be merely an estimate.

The subject of the subsequent threat assessment is the organization of the list of threats, so it is clear which threats are relevant and priority for the soft target in question. The assessment is used by executives to clarify the severity of each threat, and as a basis for the decision-making process when identifying priorities, and what security measures to take to mitigate or eliminate them. It should also be noted that it is not always possible to prevent an attack, as there is always some residual risk.

Summary of the soft target threat (degree) assessment procedure

Stage 1

- definition of **what we want to protect** (in the case of soft targets we protect human life and health);
- definition of **persons, their groups** or organizations representing a **potential threat of an attack** (sources of threat);
- definition of **expected methods of attack** by these persons or groups of persons;
- a summary of the above for **a list of possible methods of attack** on a particular soft target;

Stage 2

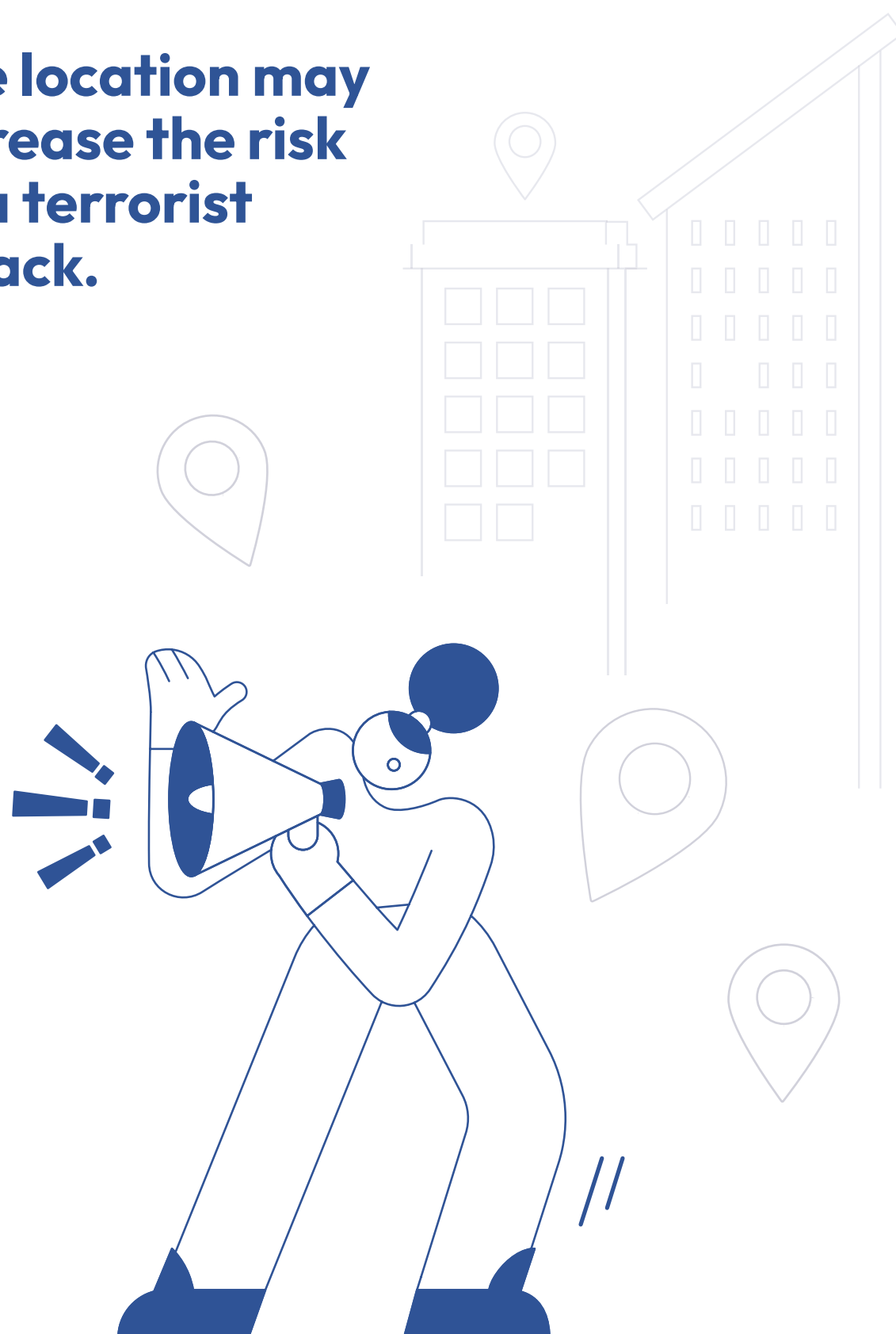
- determination of possible **attack locations and attack times** for each method of attack from the list;

Stage 3

- determination of the probability of the above-defined methods of attack (depending on the availability of means of attack, frequency of occurrence of the method of attack, the complexity of the execution of the method of attack);
- determination of the impact of the above-defined methods of attack (depending on the degree of impact on life and health, the impact on the site, the financial impact of the attack and the impact on the community);
- determination of the overall degree of threat of a particular soft target by the above-defined methods of attack

¹ Conception of Soft Target Protection for the period of 2017 - 2020, Ministry of the Interior of the Czech Republic, Prague 2017

The location may increase the risk of a terrorist attack.



Sources of threats to soft targets

Given that the correct identification of **the sources of threats** (people and their groups or organizations that are potential attackers) is essential for their assessment, we will dedicate the following chapter to it.

As mentioned above, we can protect, for example, persons, property, information, reputation. In terms of soft target protection, we will focus on the protection of persons, specifically on the **protection from violent attacks, i.e., lives and health**. For a better understanding, let's take an example of a model hospital: values (assets) that we protect in the hospital can be the people in the hospital, eventually also the property of the hospital or information that the hospital works with (personal information of patients, unique procedures), but also its reputation or good relationships (with clients, founders, donors).

Possible sources of threats to soft targets in the Czech Republic (i.e., persons and groups of persons):

- violent persons involved in classic criminal activity;
- mentally ill persons;
- avenging employees or clients;
- organized crime groups;
- extremists and hate attackers (perpetrators committing the so-called hate crime);
- terrorists.

Ordinary crime, attacks by mentally ill persons and attacks from personal vengeance cannot be excluded in any environment. In the protection of soft targets, we are concerned only with the area of personal protection by protecting against serious violent and terrorist attacks. To assess whether a particular soft target can also be a target of organized crime, hate attacks or terrorist attacks, external and internal contexts of the target must be evaluated. It is mainly its symbolism, persons present, subject of activity and the environment or previous incidents. In this context, it is necessary to highlight that terrorist attacks must be considered particularly regarding the site where the soft target is located. For example, a small restaurant, if located on the main tourist promenade, can be targeted as well as a large sports stadium.

It is advisable to analyse the given sources of threats that are relevant to a particular soft target and to try to identify as precisely as possible the specific group or individuals who can attack that particular soft target. Open-Source Intelligence (OSINT) should be used for this activity. Thus, obtaining the necessary security information about persons and groups from open sources, including social networks. Even if the soft target does not have the possibilities and funds to carry out this activity systematically and in the long term, those responsible for developing security measures should specify the sources of threats (persons and groups of persons) based on existing knowledge and experience. We can include an example of a model school:

Table 1: Demonstration of sources of threats on the case of model elementary school.

Source of threats (persons, group of persons)	Specification of the source of threats
Violent persons without ideology	e.g., attacks by mentally ill persons or revenge attacks
Organized crime groups	e.g., presence of children whose parents may be blackmailed or intimidated for their activities
Extremists and hate attackers (hate crime)	e.g., link between a school or its staff and students to political symbols or a particular ethnic or religious group (e.g., typically Jewish venues).
Terrorists	e.g., international character of the school, the link of the school or its staff and students to political or religious symbols (or the location of the school in the tourist center, in the neighbourhood of symbolically attractive buildings).

Methods of attack for individual sources of threats

The specific ways in which attacks occur vary between individuals or groups of people (sources of threats) and over time. Not only will the method of attack by terrorist organizations differ from those by organized crime groups, but there will also be differences between the methods of attacks of individual terrorist groups, racist groups, etc. Moreover, the whole situation changes over time. Therefore, it is not possible to define a general list of threats that would be valid for all soft targets, often even for individual categories (e.g., a universal list for hospitals, schools, etc.). In case such lists appear, they are of indicative use only, and it is always necessary to reassess them in relation to a particular soft target (at a given time and place).

With some exceptions, soft targets in the Czech Republic do not have adequate staff and resources for the clarification of specific sources of threats and particular threats; this methodology provides **an indicative list of methods of attacks from which it is possible to proceed**.

The source of the basic set of methods of attack that is relevant to all soft targets is mostly a violent activity associated with classic crime, violent attacks of mentally ill persons and attacks by staff or clients (basic list):

- attack with a cold weapon (stabbing, cutting, blunt weapon, etc.);
- firearm attack (short, long);
- arson attack;
- hostage-taking and barricade situation;
- attack of a soft target by a crowd (violent gatherings);
- explosive in the mail;
- toxic substance in the mail;
- setting up an explosive imitation;
- false notification of the location of an explosive (or other dangerous substances).

In addition to the basic list, the following methods of attack should also be considered in case the soft target is also attractive to **organized crime groups**:

- explosive in a parked vehicle;
- kidnapping.

In case the soft target is attractive for **racist and other hate attacks**, it is appropriate to extend the basic list with the following attacks:

- physical attack in the vicinity of the premises (especially of persons attractive for their symbolism to the attackers);
- verbal aggression (by individuals or groups) with derogatory elements and a potential to outgrow into physical violence in the vicinity of the premises.

Moreover, if the soft target is also attractive to **terrorists**, it is then appropriate to expand the list to include the following possible methods of attack both inside and in the vicinity of the site:

- suicide attack using explosives;
- a vehicle-ramming attack with an explosive with a suicidal attacker;
- a vehicle-ramming attack into a crowd of people.

The above threat guidelines represent a default set of attacks that must be taken into account. Thus, they are a tool reflecting on what kind of violence may threaten a particular soft target. They are not and cannot be an exhaustive overview of the methods of attack or an unchanging list of imminent threats to a specific soft target. At the same time, we emphasize the **need to consider other methods of attack individually for each analysed soft target**.

Creating a list of possible methods of attack on a specific soft target

The next step in the assessment is the setting of possible methods of attack into the environment of a specific soft target and establishing various variants of their possible execution. The basic way is to consider each method of attack in terms of a potentially **vulnerable place and timing**. Where and at what specific location could the given method of attack take place concerning its operational regime and security? And at what time of the day (week), or during which phase of an event?

With these considerations, it is important to empathize with the attacker and take advantage of existing experience and knowledge about attackers and their actions. Based on this, it is possible **to analyse each method of attack in several variants of execution in successive steps, and, therefore, get a better idea of where security measures should be prioritized**.

Attack localization variations

It is appropriate to start from the analysis of the characteristics of a given site and soft target context to determine the location of the attack. If the site does not have a security specialist who would perform such analysis, then we recommend considering the following basic spots in particular in terms of the location of the attack:

If it is a **facility**:

- inside the facility – all publicly accessible spaces;
- inside the facility – areas dedicated to

- important persons (whether publicly accessible or not);
- at the main entrance/security check at the entrance to the facility;
- at the supply entrance (rear, alternative);
- in close proximity of the facility (e.g., at the gates), in the vicinity of the site.

If it is an **outdoor event** (running race, gathering, etc.):

- in the center of attention (e.g., stage, starting line, finish line);
- in the crowd;
- by entrances;
- in the vicinity.

Variations of attack timing

In addition to the different variations of attack localization, different timing of the attack should also be considered. Again, it is appropriate that timing variations were determined based on site and context analysis for each soft target specifically and not merely on an assumed list created for another soft target. The key to determining relevant timing variations is the knowledge of the **regime of the site or event and the occurrence of people at different times of the day**.

Therefore, we recommend considering and completing the following attack timing variations according to the specific needs of each soft target:

- during daytime operation, when the site is open to the public;
- during the arrival and departure of a large number of personnel/public/students;
- during the organization of events for the public that are prepared beyond

- the regular regime of the facility;
- at night when the facility is not in operation².

As regards security measures of publicly accessible events (running race, gathering, etc.):

- during the preparation of the event (e.g., transport of the technical equipment, preparation of the stage, the route, etc.);
- on arrival of persons;
- during the opening ceremony (e.g., starting shot at the marathon);
- during the event;
- during the main program (e.g., especially symbolic events, the performance of a VIP guest);
- at the end (e.g., race finals, closing ceremony);
- upon termination and departure of persons.

Soft target threat (degree) assessment

A set of data is prepared to assess the vulnerability using the above balance sheet. At this point, it is already clear what **sources of threats** (persons, groups) are relevant to the given target, and **how** these sources can attack a particular soft target, in variations depending on the specific location and time of each considered attack.

Two main variables need to be identified: the **probability** that a given variation of each attack can occur, and the **impact**, that

² Only relevant for certain targets where the relevant number of persons remains at night or where there are increasingly vulnerable persons, e.g., the organization's management; it typically applies to a symbolically significant target.

such an attack would have on the given target in case it took place.

By evaluating these two variables, the soft target determines the overall **degree of threat** of a violent attack.

We will examine both the probability and impact using the scored subcategories, which will be discussed below. The measurement method may vary. In this study, we will present a technique that is used in practice for some sites that are at extreme risk³. At the same time, it is easy to process. In addition, we will offer some exemplary overall assessments at the end of this chapter, which can be used as templates and then be adapted to a particular soft target.

The point of scoring is to compare the probability and impact of each method of attack on a given target. Thus, enabling to prioritize the use of various methods of security rationally, or to reasonably decide in which priority to invest. The goal is not to attempt to calculate statistically how, when and where a target will be attacked. Exact mathematical predictions of violent attacks are only possible in practice in a limited number of specific cases. There is no general exact formula for such calculation. Experience has shown that **the most significant benefit is the actual reflection (i.e., actually answering a series of crucial questions) over each method of attack and its modelling on a protected site**.

³ The principles of the methodology presented here are based on and developed by the approach of Israeli security experts Arye Kasten and Uzi More. The method is used both by governmental organizations and the private sector (e.g., M.I.P. Security company). Software by the Resolver company is based on the same principle of threat assessments through determining the probability and impact of an incident, which is used by several governmental, educational, and health organization.

This procedure will reveal a number of significant findings that should be noted for the subsequent establishment of a soft target security strategy, and the selection of appropriate measures. Whether or not the order of attacks comes out differently is not critical.

Don't underestimate the vulnerability assessment.

Therefore, we warn against the urge to complicate the assessment procedure by attempts to calculate the exact probability or vice versa against the urge not to carry out a threat assessment at all and instead trying to apply measures to secure the soft target only based on an estimate.

Determining the probability of a given method of attack

The **probability** that a given method of attack will occur (in each examined variation of localization and timing of the attack) can be determined by assessing several subcategories. The basic ones we always recommend to consider are:

- availability** of sources of a given method of attack;
- the occurrence** of a given method of attack;
- the complexity** of execution of a given method of attack.

We evaluate these subcategories by a qualified estimate on a scale of 1–7, as shown below.

Availability of means of attack

When assessing availability, we focus on the **weapon used or other means of attack**⁴. For the assessment, it is necessary to consider whether one element or more is used (e.g., one knife or a combination of a vehicle and an explosive). Furthermore, we try to determine whether it is a weapon that can be used by anyone or whether some training or exercise is necessary (i.e., a vehicle-ramming attack into a crowd of people compared to sniper rifle attack). We also take into account whether the weapon is freely available or needs any permission (e.g., a gun) or cannot be obtained legally. The last factor to be considered for availability is delivery time – how long it is necessary to wait for a weapon, whether it is a commercially available item or a weapon that is difficult and time-consuming to obtain. Availability is assessed by a qualified estimate on a scale of 1–7 with 1 being an attack with the least available weapon and 7 being an attack with the most accessible weapon.

Table 2: Indicative scoring scale of weapon availability

7	without a weapon
6	a commonly available (e.g., knife)
5	more weapons commonly available a weapon available (e.g., car)
4	a weapon on permission or more such weapon (e.g., firearm)
3	a weapon obtainable by criminal activity (black market, etc.) without the need for professional training

⁴ In accordance with Section 118 of the Criminal Code (Act No. 40/2009 Coll.), a weapon shall be considered anything that may render an attack against a body more vigorous.

2	a weapon obtainable by criminal activity requiring professional training with delivery time
1	a weapon obtainable by criminal activity requiring professional training with delivery time

The occurrence of the method of attack

By assessing the occurrence, we determine how popular is a given method of attack on a given target **by various attackers** (groups of attackers) in each location, at the time considered. We consider whether it is an attack that has already taken place in a similar target, or whether it was in the preparatory phase. Or whether it is an attack that did not happen but took place in a nearby region, a neighbouring country, or whether it is only a hypothetical threat that is quite exceptional both here and in other regions. We rate the attraction with a qualified estimate on a scale 1-7, where 1 is the lowest frequency attack, and 7 is the highest frequency attack.

Table 3: Indicative scoring scale of occurrence of a given attack mode for a given attacker (group)

7	It has occurred many times in the Czech Republic
6	It has occurred many times, in relevant foreign countries
5	It has occurred several times in the Czech Republic
4	It has occurred several times in relevant foreign countries
3	It has occurred sporadically in the Czech Republic
2	It has occurred sporadically in relevant foreign countries
1	It has never occurred in the Czech Republic or relevant foreign countries

Note: By relevant foreign countries, we mean **Europe and its immediate surroundings**. First of all, according to empirical experience, the methods of attacks are transferred to the European territory, e.g., from the Middle East, and, second of all, free movement/exchange of persons, extremist propaganda contributing to radicalization, and sharing of information on methods of attack.

The complexity of a given method of attack

In assessing the complexity, we focus on the complexity of attack preparation, but also on the regime of the facility and its security against specific attacks carried out at a certain time in a specific location. We assess whether an attack must be prepared by an individual, group or a broader organization. Also, we consider whether it requires short-term or long-term cooperation of persons during preparation, whether the attacker must cooperate with criminal or terrorist groups when obtaining weapons or other means of attack, and whether such collaboration is one-off (e.g. acquiring an illegal gun on the black market or monitoring the facility), or it is a long-term cooperation (e.g. cooperation during collecting of information about a given target) moreover, whether it requires an intrusion into the target's regime environment or takes place in a publicly accessible location. Whether it requires its execution within a limited timeframe, at a specific location, or whether its successful execution is possible for more extended periods at several places. Complexity is assessed by a qualified estimate on a scale of 1–7, where 1 is the most sophisticated attack and 7 is the most easily feasible attack.

Table 4: Indicative scoring scale of **complexity** (consider the real functionality of the security elements for each method of attack considered)

7	an individual without the assistance of other people, publicly accessible place
6	requires the involvement of several people, publicly accessible place
5	simple or one-time cooperation with a local criminal group, publicly accessible place
4	more complex or longer-term cooperation with a criminal group, place inaccessible to the public
3	one-time cooperation with a local terrorist group, place inaccessible to the public
2	coordinated action at local level in cooperation with a terrorist group, place inaccessible to the public
1	an internationally coordinated, long-term action by a terrorist group, publicly accessible or inaccessible place

Sample evaluation of resource availability, occurrence and complexity of the attack

The assessment of factors as regards the availability of the means of attack and occurrence of methods of attack is for all targets in the Czech Republic similar. These factors focus on weapons, preferences of dangerous groups and methods of attack, not on the specifics and vulnerability of a specific attack target.

This is in contrast to the attack complexity factor, which will vary according to the specifics of each target. Therefore, to facilitate the work with the assessment, we present a sample assessment of availability and occurrence of specific methods of attack that should always be reassessed with regard to the location, timing and long-term development. As an example, we chose the probability assessment concerning methods of attack by right-wing radicals that is well-conceivable in the Czech Republic.

Table 4: Sample assessment of resource availability and occurrence for selected methods of attack in relation to the meth-

ods used by **right-wing radicals** (we recommend reconsidering and adjusting each value for each specific target).

Identification of impending methods of attack	Probability		
	Availability	Occurrence	Complexity
Attack with a cold weapon (stabbing, cutting, blunt weapons, etc.)	6	7	7
attack with a firearm that is available only illegally	4	3	5
Arson attack	3	3	5
Hostage-taking and barricade situation	6	6	7
Attack on a soft target by a large group or crowd (violent gatherings)	6	2	7
Explosive in mail	6	5	6
A toxic substance in mail	3	6	7
Suicide attack using explosives	3	6	7
Explosive in a parked vehicle	2	2	6
Vehicle ramming attack with an explosive with a suicidal attacker	3	2	6
Vehicle ramming attack	2	2	6
Verbal aggression (individuals and groups) with the potential to grow into violence	5	4	7
Physical attack by an individual (small group) without using a weapon	7	7	7
Attack using explosives (without the presence of an attacker)	7	7	7
útok s použitím výbušniny (bez přítomnosti útočníka)	3	4	5

The total probability of a given attack method is then obtained by summing the availability, occurrence, and complexity values. Thus, the highest value of the overall probability of a particular attack method can be 7+7+7=21. This is how we then determine the probability for each of the expected attack methods.

Impact assessment

By impact in this section, we mean the negative effects that an attack would have on a protected soft target. By definition, the attack will, of course, aim at lives and health (we address attacks on soft targets), but even an attack with this aim will usually have several impacts on values other than life and health. Therefore, we must also include other values in the impact assessment. Similarly, to probability, we will examine the impact by using subcategories. Commonly, subcategories are set by each soft target individually, because it focuses protection on various protected interests („assets“). In this document, we will, therefore, focus on basic subcategories that should always be considered. These are:

- impact on life and health;
- impact on the facility;
- financial impact;
- impact on the directly affected community.

We evaluate these subcategories as in the case of probability with a qualified estimate on the scale 1–7, as shown below. In many cases, the more precise impact assessment is determined by circumstances that cannot be predicted. Impact assessment is a matter of expertise and experience even more than in other categories.

Nevertheless, we recommend that you also define the impact in layman’s terms. It is always possible to request an expert impact assessment. **Again, it is emphasized that the purpose of the assessment is not to have an exact table with figures, but to reflect on the various methods of attack, to systematically reveal weaknesses or areas of the unknown that are appropriate to explore further.**

The purpose of the evaluation is to identify weaknesses and unknowns.

Impact on lives and health

In assessing the impact on lives and health, we focus on the number of people who can be affected by the attack in each variant (at a given time and place) and the severity of the consequences on life and health.

Table 5: Indicative scoring scale of impact on lives and health

7	severe injuries of a larger number of people and deaths of a larger number of people
6	severe injuries of a larger number of people and deaths of a few individuals
5	several injuries of a larger number of people
4	several injuries of a few individuals
3	minor injuries of a large number of people
2	minor injuries of a few individuals
1	shock, or minor injuries

Impact on a facility

By assessing the impact on a facility, we **not only focus on the technical damage to the building but also on the impact of the attack on its operation as well as the possibility to continue its operation after the attack.**

Table 6: Indicative scoring scale of impact on a facility (event)

7	destruction of the building or disruption of statics cancellation of an event
6	extensive restriction on the functionality of the building or the possibility to organize an event
5	restriction on the functionality of a part of the building or a part of an event
4	local restrictions on the functionality of a room or a part of an event
3	significant damage to the building or disruption of an event without restrictions on the functionality
2	minor damage to the building or disruption of an event without restrictions on the functionality
1	no or negligible damage to the building or disruption of an event

Financial impact

There are several levels of impact on the economy. It is up to each entity to choose to measure short-term impact associated with reconstructions, short-term restriction to its operation, etc. Or whether it will also consider the long-term impact on attendance, economy of the affected location, etc. In this type of assessment, we particularly emphasize the need to adapt it to the specific soft target situation and the financial capabilities of its manager (e.g., what will have a liquidation impact will be different at a shopping center and a small NGO).

Table 7: Demonstration of possible scaling (scoring needs to be adjusted for each target to match (e.g., economic) conditions of the given soft target)

7	economically liquidation impact
6	impact over CZK 500.000 not covered by insurance
5	impact over CZK 100.000 not covered by insurance
4	impact over CZK 100.000 covered by insurance
3	impact in dozens of thousands CZK
2	impact up to 5.000 CZK
1	without impact, possibly negligible

Impact on the functioning of the affected community

The assessment of this impact focuses on the effects of an attack on a community that was directly affected by the attack. This may refer to a community of a school, consisting of pupils, parents and teachers, or company personnel affected by the attack, or a religious, ethnic, or other groups.

Table 8: Indicative scoring scale of impact on the functioning of the community

7	termination of participation n/activity
6	temporary suspension of activities
5	the real risk of endangering people when participating in other activities
4	general concern to be active in the community, more significant restrictions on activities
3	minor restrictions of activities
2	weak impact at an individual level
1	without any apparent impact on community

Method for calculating the impact rate on a soft target

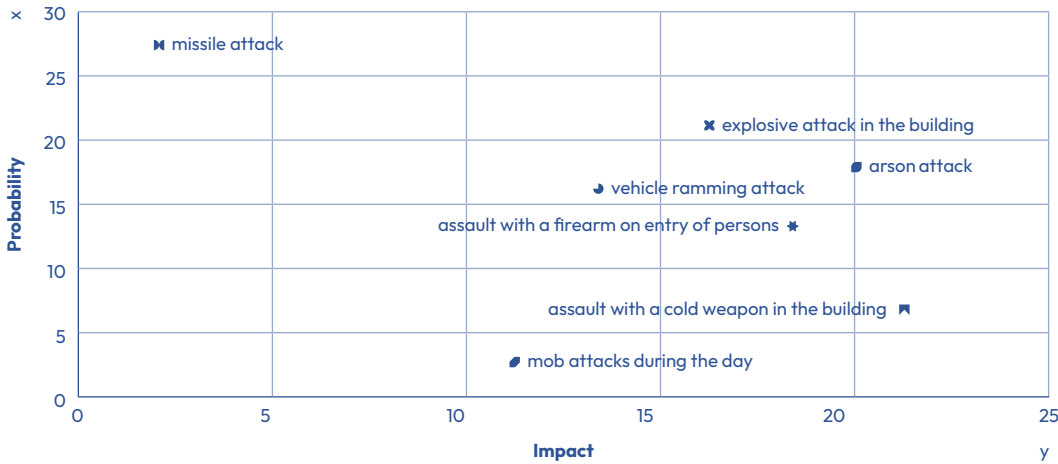
Unlike some probability subcategories, impact assessments will vary for individual soft targets. It is, therefore, not appropriate to provide sample tables with values.

However, we calculate the total value of the impact of the attack by summing the impact values on life/health, finances, community functioning, or a facility (event). Thus, the highest total impact rate may be 7+7+7+7=28.

Assessment of the overall threat level

The resulting values of probability and impact of a particular method of attack are entered into the graph. The higher the intersection of the probability and impact values on the x-axis, the higher the impact will be. The higher the intersection of the probability and impact values on the y-axis, the higher the likelihood of a given method of attack.

Graph 1: Demonstration of graphical representation of values for probability and impact



The vulnerability rate helps to compare and prioritise attacks.

In addition to adding data to a graph, it is appropriate to calculate the overall threat degree by multiplying the total probability value and the total impact value. With this level of vulnerability, it is then possible to compare and prioritize attacks.

Total degree of vulnerability = total probability x total impact

For a better idea, here is an example concerning a model high school.

Probability and impact values of attacks are plotted on a graph and multiplied to calculate overall threat level for comparison and prioritization.

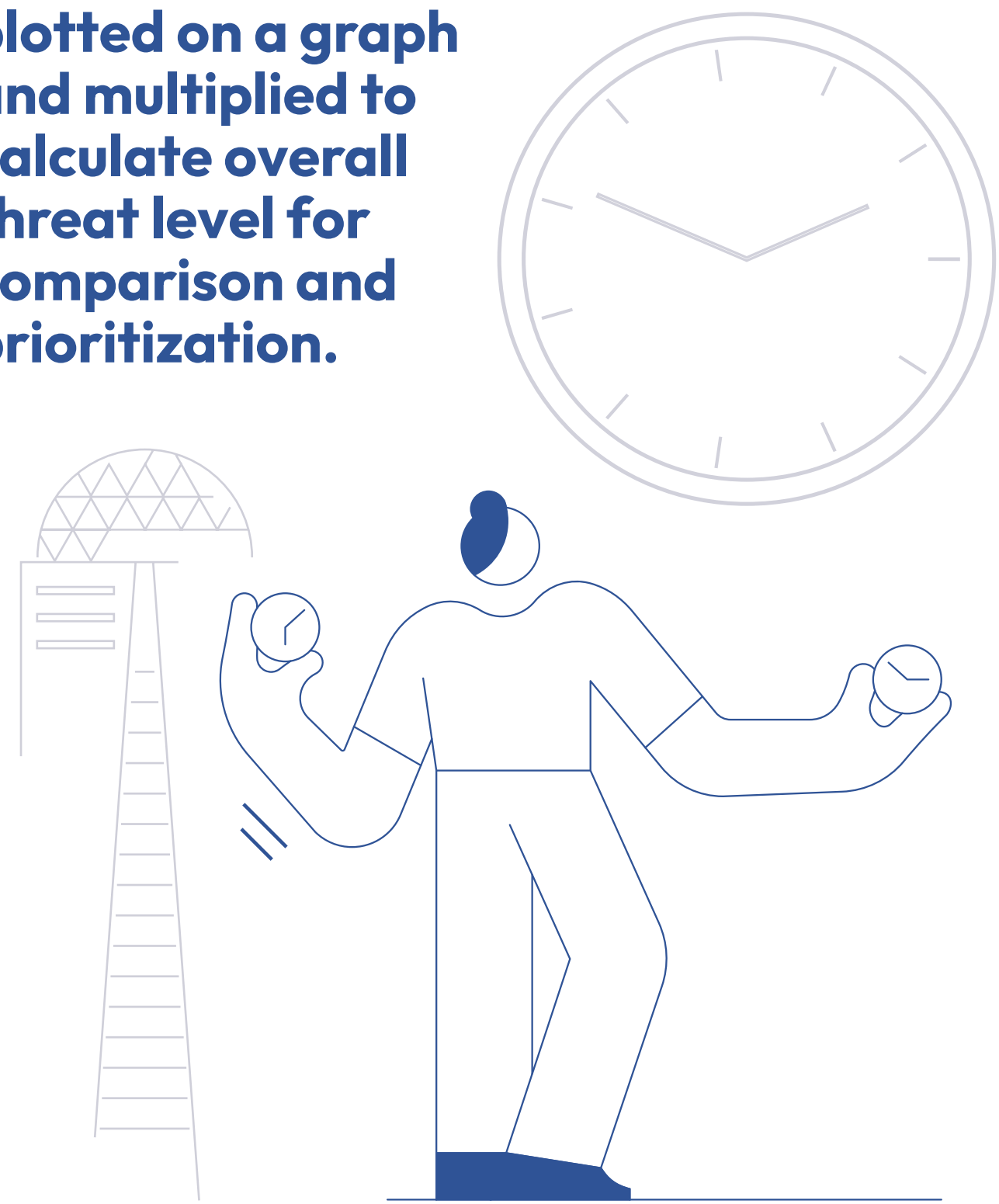


Table 9: Example of total values for probability, impact and degree of vulnerability of a model high school (numerical values entered into the table are used from one assessment of a particular school in the Czech Republic)

Identification of imminent methods of attack	Localization	Timing	Assessment		
			Sum probability	Sum Impact	Total degree of vulnerability
Arson	inside	at night	19	16	304
Violent attack with a firearm	inside	during classes	14	17	238
Violent attack with a firearm	on the premises in the areal	on arrival	14	15	210
Violent attack with a firearm	on the premises	during classes	14	13	182
Violent attack with a cold weapon	on the premisesl	during classes / on arrival and when leaving	19	9	171
Violent attack with a cold weapon	in front of the premises	during classes / on arrival and when leaving	17	7	119
Violent attack with a cold weapon	inside	during classes / on arrival and when leaving	18	9	162
Attack with the use of explosives	inside	during classes claclasses	5	20	100
Attack with the use of explosives	In front of the premise	on arrival / when leaving	6	18	108
Hostage and barricade situation	inside	during classes	10	13	130
Violent attack of low intensity	Inside / on the premises	during classes / on arrival and when leaving	21	5	105

The obtained values can then be used to compare the vulnerability at different locations or at different times of the day. It is necessary for the subsequent draft of the system of security measures, as one method of attack may require something completely different should it happen at the entrance at the time of arrival of persons to the facility or in front of the facility during the day.

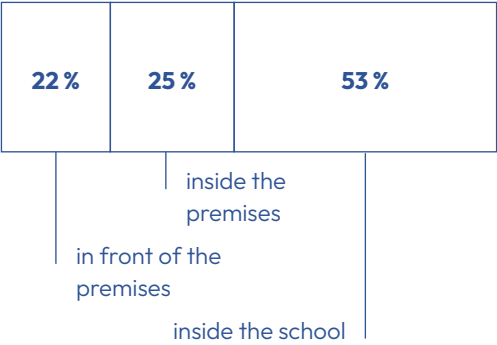
To compare the distribution of threats to the model school as mentioned above, we proceed by adding the threat values for attacks considered inside the facility. Next, we sum up the vulnerability values for the attacks considered **inside the premises** and finally, **in front of the premises**. The procedure is shown in the table below, where for simplicity, we only list some of the above-given attacks.

Table 10: An example of the calculation of the threat level for each considered **localization**

identification of imminent modes of attack	Localization of threat		
	Inside the school	On the premises	In front of the premises
Arson	304	/	/
Violent attack with a firearm	238	210	182
Violent attack with a cold weapon	162	171	119
Attack with the use of explosives	100	/	/
Hostage and barricade situation	130	/	/
Violent attack of low intensity	105	105	105
Localization of threat	1039	485	427

For a better overview, the values can be expressed graphically. It is then possible to clearly identify when and where attacks may take place and where attention needs to be focused.

Graph 2: An example of the ratio of localization of a model school's threat

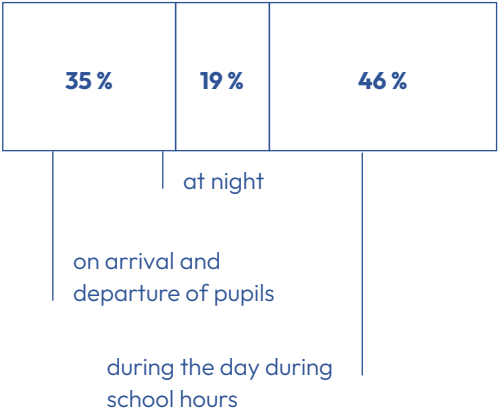


Similarly, it is possible to analyze the timing of examined attacks and their level of vulnerability.

Table 11: An example of the calculation of the threat level for each considered timing of selected attacks at a model school.

Identification of imminent attack methods	A threat level at different times of the day		
	At night	During the day during classes	On arrival/ departure of pupils
Arson	304	/	/
Violent attack with a firearm	/	238	182
Violent attack with a cold weapon	/	171	171
Attack with the use of explosives indoor	/	100	108
Hostage and barricade situation	/	130	/
Violent attack of low intensity	/	105	105
Threat timing	304	744	566

Graph 3: An example of the timing of a model school's threat



Conclusion

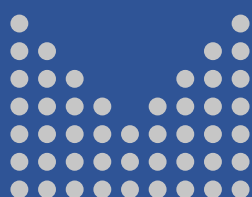
By evaluating the probability and impact of an attack, we can better understand when and where we face a threat of a specific attack. By calculating the threat rate and examining it, it is then possible to identify when and where our attention should be focused. The idea is to target security measures effectively to places and times when relevant attacks threaten us.

This assessment shall be followed by **a proposal for a system of security measures. The methodology for elaborating this proposal is not the subject of this publication.** A proposal for such a system can be designed in several ways. However, it should always be a systematic, methodical procedure, based on probability and impact assessment, seeking appropriate security measures for a) deterrence of attackers or other prevention of attacks, b) their timely detection, c) a prompt response, and d) mitigation of the impact of the incident.¹

¹ Thus, according to the known acronym DDRM (detect, deter (prevent), react, mitigate).

Assessing threat likelihood and impact guides effective, tailored security measures—avoiding generic or poorly integrated solutions.





MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

Soft Target Threat Assessment

or what, when, where and from whom you are threatened

2nd revised edition

www.mv.gov.cz