



## Mieczysław Bieniek

Associate Professor, Andrzej Frycz Modrzewski Krakow University  
<http://orcid.org/0000-0002-6993-7606>

# ‘Soft Targets’ Protection Awareness: A Case for Specialized Security Education Need<sup>1</sup>

## Introduction

Various threats of the contemporary world call for effective protection realized by fighting against terrorism and organized crime, strengthening defense, and building resilience. The key areas here are information systems and interoperability, soft target protection, and cyber threats.

The lack of information systems’ interconnectedness and the fact that data is not systematically fed into the relevant bases by NATO and EU member states are weaknesses in the Security Union’s practical implementation. Close cooperation between EU countries is the way to change this.

Despite our successes, the terrorist landscape grew more complex in 2017. ISIS, al-Qa’ida, and their affiliates have proven to be resilient, determined, and adaptable, and they have adjusted to heightened counterterrorism pressure [...]. They have become more dispersed and clandestine, turning to the internet to inspire attacks by distant followers, and [...] have made themselves less susceptible to conventional military action. Further, the return or relocation of foreign terrorist fighters from the battlefield has contributed to a growing cadre of experienced, sophisticated, and connected terrorist networks [...].<sup>2</sup>

<sup>1</sup> The conference ‘Soft target protection in a conflict area’ took place in Prague on 28–30.05.2019. The conference was held as a part of NATO’s Science for Peace and Security Programme.

<sup>2</sup> Country Reports on Terrorism 2017, U.S. State Department 2017, <https://www.state.gov/reports/country-reports-on-terrorism-2017> [accessed: 10.12.2021].

Typically, soft targets are locations easily accessible to the general public and particularly vulnerable to attacks. As they are difficult to protect, an attack on soft target has a high probability of involving mass casualties. The risk of further attacks on soft targets, including transport, remains high, as evidenced by available studies, including the Europol report on changes in the way Islamic State operates.<sup>3</sup> Terrorist groups choose to strike almost exclusively soft targets.

Typical soft targets include:

- educational facilities;
- religious sites and places of worship;
- commercial facilities;
- entertainment venues;
- gatherings, parades<sup>4</sup>, demonstrations (AL-SADAT in Egypt in 1981 during a parade);
- bars, clubs, dance clubs, restaurants and hotels (Berlin, Paris, Kabul, Baghdad);
- locations important for recreation and tourism;
- sporting arenas and stadiums (Paris);
- transportation sites (London, Brussels, Madrid);
- healthcare facilities;
- public meetings, pilgrimages, fairs (Karbala, An -Najaf);
- community centers.<sup>5</sup>

The term *soft target*

has typically been used to describe locations that are easily accessible and predominantly civilian, often with limited security measures in place. These types of locations have long been preferred targets of attacks – they provide terrorists with an opportunity to maximize casualties and generate widespread publicity. Recent research has given more insights into the targeting methodology. One global study has concluded that, in 2017, an average of 17 civilians per day were killed by terrorist attacks, often as a direct result of coordinated campaigns. Another study has found that “soft-civilian targets” were the predominant focus of suicide attacks conducted by Boko Haram between 2011 and 2017.<sup>6</sup>

In conflict zones, the line between a perceived enemy state and that state’s general public is easily blurred through a group’s ideological rationale, which is often reduced to ‘us and them’.

---

<sup>3</sup> EU Terrorism Situation and Trend Report (TE-SAT) 2017, <https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017> [accessed: 10.12.2021].

<sup>4</sup> M. Hoffman, *Egipskatragedia*, <https://www.mowiaiwieki.pl/index.php?page=artykul&id=1015> [accessed: 10.12.2021].

<sup>5</sup> *Basics of soft targets protection guidelines*, Prague 2016, <https://www.mvcr.cz/cthh/soubor/basics-of-soft-target-protection-guidelines.aspx> [accessed: 10.12.2021].

<sup>6</sup> *UN CTED Analytical Brief: Responding to terrorist threats against soft targets*, 16.09.2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf> [accessed: 10.12.2021]; J. Warner, H. Matfess, *Exploding Stereotypes: The Unexpected Operational and Demographic Characteristics of Boko Haram’s Suicide Bombers*, Combating Terrorism Center, 9.08.2017, <https://ctc.usma.edu/report-exploding-stereotypes-the-unexpected-operational-and-demographic-characteristics-of-boko-harams-suicide-bombers> [accessed: 10.12.2021].

Although targeting security forces may also result in civilian fatalities, the focus here is on violence intended to harm civilians.

Soft-target attacks can appear senseless and chaotic, designed merely to spread fear and maximize damage. Such violence is inherent to many Islamist militant organizations. However, analysis has revealed distinctions in the systematic killing of unarmed civilians and the targeting of vulnerable institutions.

By recognizing both the scale of this terror and the differences between the perpetrators, front-line responders can better counter this violence. In my view, Islamist militant violence overwhelmingly affects Muslim civilians. Extremist organizations have complex sectarian and religious prejudice shaping their use of violence. There are important distinctions in the methods and justifications for killing civilians. Sectarian, political, and social factors determine the degree of a group's campaign against the public. Similarly, access to resources and financial capacity can affect the efficacy of a group's violence towards civilians. However, all of these groups espouse a hard-line narrative, drawing on an extreme interpretation of Islam that permits the targeting of civilians.

Beyond violence, extremist groups are strategic about the propaganda and messaging surrounding the assaults on civilians. Militant groups have condemned attacks in the public space that were carried out by other groups. By exploiting the public outrage, extremist groups attempt to position themselves as authoritative leaders in the Islamist landscape.

Islamist militant groups are aware that attacks on civilians may hinder their goals and capacity to appeal to the public. Groups have become adept at tailoring their post-assault communication to control the narrative and uphold their reputation.

Violent extremist organizations have claimed that the collateral killing of Sunni Muslims is acceptable because such victims will enter into heaven as martyrs. The perpetrators have manipulated the disputed Islamic concept of *takfir*,<sup>7</sup> the act of one Muslim declaring another to be a non-believer, to legitimize murder.

Beyond the general population, there are specific targets in the public space that fall victim to Islamist extremist groups. Exploring the nature of these attacks offers a deeper insight into why extremist groups designate targets such as media organizations.

Such an understanding shows the significant effect violence has on these sectors and allows for a greater focus on protecting the public space. The targeting of particular sectors of society has detrimental effects on the public. It erodes public confidence and fosters fear among populations.

Extremist groups portray the media industry as representing secular and Western values (freedom of speech, human rights).

The industry is seen as antagonistic to the binary and absolute worldviews of Islamist extremist teachings.

Islamist extremist groups launched attacks on educational institutions. The targets included teachers and school facilities.

---

<sup>7</sup> G.H. Rassool, *Islamic psychology. Human Behavior and Experience from an Islamic Perspective*, London–New York 2008, [https://iou.edu.gm/wp-content/uploads/2021/04/IslamicPsychology\\_HumanBehaviour\\_ch1.pdf](https://iou.edu.gm/wp-content/uploads/2021/04/IslamicPsychology_HumanBehaviour_ch1.pdf) [accessed: 10.12.2021].

The types of professionals attacked included bank workers, judges, doctors, business people, and lawyers. Laborers comprise various infrastructure workers, including people who work for gas and water companies, farmers, traders, and telecommunication workers.

Governments could be considered hard targets, as they are often militarized and protected by armed forces. However, Islamist extremists reason that attacking government figures can fulfill wider strategic aims. The targets include government staff and buildings.<sup>8</sup>

A serious commitment to specialized protection training is crucial in building up and managing a protection response on behalf of soft targets. Staff training programs should include protection components in seminars and workshops in addition to courses specifically on protection issues.

A systematic approach to protection training should include:

- coordination of efforts;
- identification of protection-training needs;
- design and development of the training modules;
- methods for delivering training and evaluation;

Protection training should incorporate several different components:

- training before deployment, particularly for first-mission humanitarian workers;
- training and orientation after arrival for the mission, together with coaching by a more experienced colleague/superior;
- periodic training during the mission, including training in specific practical subjects;
- regular de-briefing at the mission end.

Protection training should achieve the following objectives:

- define the concept of protection;
- identify the legal framework applicable during a conflict, for understanding violations committed against civilians;
- design a strategy following the mandate, principles, and working procedures of the humanitarian organization;
- design an ethical strategy for collecting data related to violations;
- identify perpetrators of violence, analyze causes of behavior leading to violations, and devise correction strategies: developing the ability to deal with coordination issues and enhancing protection, understanding the mandates/capacities of other actors;
- develop skills for interacting with victims and assessing the risks they face and the resilience they have developed.

Protection training is one of the main tasks of the protection division. The protection training policy is based on identifying the required skills. To develop and enhance the professional skills of designated staff in areas related to protection activities, many courses are organized at headquarters and a field level. They should be supplemented with coaching by immediate supervisors in the field.

---

<sup>8</sup> *How Islamist Extremists Target Civilians*, 13.09.2018, The Tony Blair Institute for Global Change, <https://institute.global/policy/how-islamist-extremists-target-civilians> [accessed: 10.12.2021].

## Principles of soft targets protection

### Choosing the right security measures

I have described the prevailing forms of terrorist attacks which can inform the choice of security measures. The data help decide on the security approach, articulate the main principles of securing a target and recommend specific steps to set up an efficient security system.

These are the steps to be taken (or questions to be answered) before setting up a functional security system:

Creating a soft target security system, it is important to clarify what is to be protected. Therefore, we start by defining what are the entities of importance and what harm they may face. Common areas of protection would be people's safety, property, information, values. This Guideline primarily addresses protection from violent assaults. Nevertheless, the measures we discuss are also applicable to the disruption of public order, some types of threat to the property, or prevention of dangerous situations caused by technical accidents.

The next thing is to define potential sources of danger/threat against the protected entities. We identify particular enemy groups or categories of individuals with a conceivable motive. To do so, we need to analyze previous attacks of similar nature and to consider potential sources of threat. It is necessary to mind the specifics of the protected entity (presence of VIPs, attention of the media, high-risk timing of an event, explosives, resilience, etc.).

Accurately defined sources of threat make it possible to forecast the possible forms of attack. These two aspects are the cornerstone on which we should build a security system for a given soft target. Without a sound analysis of potential dangers, the security system will be inefficient.

The guideline is based on a systematic analysis of the threats posed to soft targets. Once the analysis is complete and the possible threats are defined, we can move on to select and implement adequate security measures.

There are several methods of analyzing threats and risks. Above all, it is important to rank the threats by likelihood of occurrence and by the seriousness of the impact. Relevant data is fed to a security threat analysis and that generates a rating list of major threats. This list helps to set up the security system and to allot resources more effectively.

Knowing the major threats makes it possible to select adequate security measures. The next phase is implementation. The phase where technical equipment is installed and where customized security plans are created. The plans must define preventive measures as well as routine procedures and responses. In case an attack can not be prevented, attackers must be stopped at the earliest possible stage and the impact must be minimized.

All security solutions designed for soft targets must be:

- of various environments and applicable to attacks by different enemies;
- fool-proof and efficient – people's lives are at stake;
- creative – the resources are usually limited;
- flexible – they must meet the needs of groups, tactics, and weapons.

## Security personnel

Guard force. Security guards can perform entrance checks and patrol. They can also be in charge of the control room and the security technology. A well-trained guard force is the most efficient security tool for deterrence, early detection, immediate response, and mitigation of impact. Security guards can be employed directly or by a private security agency. Security staff should abide by standardized procedures. The procedures must be tailored to the specifics of the premises and revised regularly. All routines must be described in detail and provide reliable guidance in case of less frequent situations. However, the procedures for security incidents need to be brief and reinforced by tactical training. The essential tool of a security guard is communication, so the training plan should always include assertiveness and crisis communication.

Other personnel. The term applies to the employees who are not directly responsible for security but who are part of the organizational structure. Such employees can be receptionists, janitors, organizers, teachers, supervisors, ushers, volunteers, or cleaners. A special role should be played by the management, who will also be trained to coordinate recovery activities during the post-incident phase.

## Electronic devices and flying drone systems

Camera surveillance systems are used to monitor interior and exterior areas. Camera surveillance systems can be constantly checked by security guards and receptionists or can serve solely as a recording device. It is advisable to monitor the entrance area in particular.

Determining the number of cameras to be installed, it is wise to take into account the number of the staff in charge. It is not recommended to show more than 4 camera views on a 17-inch monitor. Cameras should be motion-activated so dispatchers are alerted by the screen switching on. Movable cameras are less effective: trying to see everything, many end up seeing nothing at all.

Many camera surveillance systems have analytical functions, such as face detection or suspicious behavior detection. However, these analytical functions need to be operated and evaluated by qualified staff.

Security alarm systems serve primarily for the detection of perimeter intrusion or unauthorized entry. The systems are divided into perimeter, shield, spatial, object. We can name many, such as motion detectors, open door sensors, glass-breaking sensors, fence climbing detectors. In all these devices, the alarm output may be local or remote – connected to a local switchboard, sent by SMS to a mobile device, or sent out to a Surveillance and Alarm Receiving Center.

A public address system is an extremely efficient tool of communication in case of an emergency. It is recommended to have two pre-recorded announcements – one for the evacuation of the building (in case of fire) and another requesting to 'stay put' and 'lock-down'.

X-ray scanners are used to detect weapons, bombs, and explosives in baggage. An X-ray check is performed simultaneously with a metal detection check. They can

be performed randomly. Efficient use of X-ray equipment requires well-trained and regularly tested staff.

Metal detectors are available in two forms – as walk-through frames and as hand-held scanners. Both are used to detect metal weapons and metal parts in bombs. Of course, metal detectors will not detect weapons and bombs made of other materials or explosives as such. Checks can be performed randomly. Efficient use of metal detectors requires trained staff.

Explosive detectors (*sniffers*) are among the more recent and sophisticated security tools. They are demanding in terms of maintenance but relatively user-friendly. *Sniffers* are capable to detect a wider range of explosives than K-9 dogs trained to search for explosives. *Sniffers* are used mainly at entry checks or for the detection of suspicious objects or vehicles.

Entry and attendance control systems primarily provide data for the payroll office but at the same time can be used to hinder unauthorized access to and within the building. Doors and walk-ins operating on chips, cards, or biometric recognition can efficiently prevent criminal behavior and vandalism; however, they do not provide sufficient protection in case of an active attack.

ID scanners are used for identity documents' verification. Efficient use of an ID scanner requires well-trained staff.

Public emergency alerts (mobile applications, SMS portals) represent a crucial means of early warning for people within a threatened area. Personalized messages and the possibility to communicate with the dispatcher may significantly reduce tension and prevent people from entering dangerous zones.

Light (switched on by photosensors) is an underestimated component of the security system. At minimum cost, it serves as one of the most efficient means of deterrence.

## Mechanical devices

Security doors of different security ranking grades provide enhanced protection against forced entry and the overall resilience of a building's outer shield. Security doors can be bomb-resistant, bullet-resistant, and extreme-intrusion-attempts resistant. In combination with access and attendance control technology, they are an efficient tool for preventing forced entry. It is important that the frame of a security door is built into the walls; otherwise, the door is less resistant to explosions. Ideally, security doors should be a part of the original construction plan. Replacement of frames can be complicated, especially in older buildings.

Bullet-resistant, explosion-resistant, or break-resistant security windows are also an efficient component of buildings' shield protection. Same as the doors, window frames need to be firmly anchored in the walls or their resilience decreases. An alternative way to protect windows from attacks and explosions is using heavy curtains.

Fencing is a means of restricting unauthorized access to protected premises. Fencing, especially if reinforced by security alarms and camera surveillance, is an efficient tool for securing a perimeter by narrowing the access pathway.

Turnstiles are used to keep order and authorize access at an entrance and an exit. The rest of the perimeter and the outer shield of the building needs to be controlled. For security purposes, it should not be possible to climb over the turnstiles without the guards' notice. When it comes to exits, the main advantage of turnstiles is that the people exiting cannot 'hold the door' for unauthorized incomers. Turnstiles are often fitted with an ID scanner.

Bollards, concrete medians, and other mechanical barriers are used to prevent unauthorized parking (regimen measure) or access of a vehicle with a bomb (security measure). Attention should be paid to the material, anchoring, and distance of the installed devices so that the bollards cannot be bypassed or easily destroyed or removed. Barriers installed to prevent vehicles access must meet the parameters given by the estimated speed and weight of an attacking car.

## Recommendation to increase soft targets' resilience

1. Understand your security specifics. Start by identifying your security issue and the activities that might make you or the people you work with desirable targets. What are the high-risk times during the day, month, or year? Who can you assign security tasks to? Which security solutions have proven successful? Specify what would be your focus and find the strengths and weaknesses of your defense.
2. Be methodical. Your security solution must be cost-effective. Therefore, you must first clarify what kind of incidents need to be solved and only then determine which measures you want to adopt. Your goal is to be able to eliminate threats before, during, and after an incident. Clarify the purpose of each security component (both already purchased and planned). Who is going to operate it? Who will train and supervise the operator?
3. Engage local staff. Local employees can assist to prevent and detect threats, and to mitigate the impact of security incidents. Even if you do not have security guards, assign tasks and responsibilities to your employees, volunteers, assistants, "marshals" etc.
4. Focus primarily on prevention and mitigation of impact. Your task is NOT to eliminate the attacker but to prevent an attack, to detect threats as early as possible. Elimination of the attacker should be left for the police or armed security force.
5. Stick to standard procedures. Set up your plans for all relevant situations – checking visitors, documents, responding to suspicious situations, etc. Get ready for evacuation as well as invacuation. When the target seems to be under attack (shooting in front of the building, armed robbery, etc.), it is safer to stay inside the building and lock it down until the police arrive. Set up your lockdown procedures and try to identify a room that can serve as a lockable shelter – a 'safe haven'.
6. Set up a coordination plan for your management. The situation after a security incident is extremely stressful. It is necessary to make decisions and it is helpful if these measures have been taken beforehand. Responsibilities need to be assigned and actions need to be coordinated.



7. Raise your staff's security awareness. Make sure to bring forward the topic of potential threats and to revise response procedures regularly. Drill procedures from time to time.
8. Set up cooperation with your local department of the municipal police, or with other units of the Integrated Rescue System (Fire Squad or Health Care Rescue Squad). Show them around your premises, discuss potential threats, share information about special events, and consult your security plans for emergencies.
9. If you perform entry checks, look not only for weapons but also for harmful intentions. Security frames and X-rays will only detect a weapon if they are operated by well-trained and regularly tested staff. Even if there is no weapon to be found, a motivated attacker will always find something weapon-like beyond the checkpoint. Apply methods for detecting suspicious behavior and organize security interviews.
10. Take the soft target's surroundings into consideration. Securing soft targets, we must often protect an area rather than an isolated site. This is particularly true about soft targets located in close vicinity to each other.<sup>9</sup>

Education for security is a multi-faceted undertaking. It concerns not only the types of threats or ways of counteracting them, but also issues management, the use of the latest technological achievements, or psychology to protect the people at risk.

This article focuses on one specialized area of education for security: soft targets' protection. Hence it mentions the characteristics of threats and potential target locations, and finally specific solutions and guidelines. Of course, the identified methods of action are the result of sometimes painful experiences and generalizations allowing for the construction of integrated protection systems. But such a holistic approach would be impossible without security education as such. Therefore, it should apply not only to security staff. It should also be raised with the decision-makers – politicians who make strategic decisions. Moreover, average citizens should build awareness from an early age, to identify threats and learn to act properly in potentially dangerous circumstances.

If even one human life is saved as a result, it will mean that the effort put into education for security has not been wasted.

## Conclusions

To conclude, let me share a quote from Federica Mogherini, the EU Commissioner for Foreign Affairs and Security Policy:

None of our countries has the strength nor the resources to address these threats and seize the opportunities of our time alone. But as a Union of almost half a billion citizens, our potential is unparalleled. [...] And wherever I travel, our partners expect the European Union to play a major role, including as a global security provider. We will deliver on our citizens' needs and make our partnerships work only if we act together, united. This is exactly the aim of the Global Strategy for European Foreign and Security

---

<sup>9</sup> *Basics of soft targets protection guidelines*, Prague 2016, <https://www.mvcr.cz/cthh/soubor/basics-of-soft-target-protection-guidelines.aspx> [accessed: 10.12.2021].

Policy. "Global" is not just intended in a geographical sense: it also refers to the wide array of policies and instruments the Strategy promotes.<sup>10</sup>

The awareness of the threats that accompany our lives is the reason why societies should be ready to respond to them. As shown by the events of recent years, intensive training and preparation should be conducted to prevent acts of terrorism, and if they do occur – to minimize the losses.

## References

- Basics of soft targets protection guidelines*, Prague 2016, <https://www.mvcr.cz/cthh/soubor/basics-of-soft-target-protection-guidelines.aspx> [accessed: 10.12.2021].
- Country Reports on Terrorism 2017*, U.S. State Department 2017, <https://www.state.gov/reports/country-reports-on-terrorism-2017> [accessed: 10.12.2021].
- EU Terrorism Situation and Trend Report (TE-SAT) 2017, <https://www.europol.europa.eu/publications-events/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017> [accessed: 10.12.2021].
- Gierszewski J., *Organizacja systemu bezpieczeństwa społecznego*, Warszawa 2013.
- Hoffman M., *Egipska tragedia*, <https://www.mowiaiwieki.pl/index.php?page=artykul&id=1015> [accessed: 10.12.2021].
- How Islamist Extremists Target Civilians*, 13.09.2018, The Tony Blair Institute for Global Change, <https://institute.global/policy/how-islamist-extremists-target-civilians> [accessed: 10.12.2021].
- Michalczak T., *Europa w obliczu islamskiego terroryzmu. Dlaczego dochodzi do ataków terrorystycznych i jak im przeciwdziałać*, Warszawa 2019.
- Mogherini F., *Foreword*, [in:] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, June 2016, [https://eeas.europa.eu/archives/docs/top\\_stories/pdf/eugs\\_review\\_web.pdf](https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf) [accessed: 10.12.2021].
- Rassool G.H., *Islamic psychology. Human Behavior and Experience from an Islamic Perspective*, London–New York 2008, [https://iou.edu.gm/wp-content/uploads/2021/04/IslamicPsychology\\_HumanBehaviour\\_ch1.pdf](https://iou.edu.gm/wp-content/uploads/2021/04/IslamicPsychology_HumanBehaviour_ch1.pdf) [accessed: 10.12.2021].
- UN CTED Analytical Brief: Responding to terrorist threats against soft targets*, 16.09.2019, <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf> [accessed: 10.12.2021].
- Warner J., Matfess H., *Exploding Stereotypes: The Unexpected Operational and Demographic Characteristics of Boko Haram's Suicide Bombers*, Combating Terrorism Center, 9.08.2017, <https://ctc.usma.edu/report-exploding-stereotypes-the-unexpected-operational-and-demographic-characteristics-of-boko-harams-suicide-bombers> [accessed: 10.12.2021].

---

<sup>10</sup> F. Mogherini, *Foreword*, [in:] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, June 2016, [https://eeas.europa.eu/archives/docs/top\\_stories/pdf/eugs\\_review\\_web.pdf](https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf) [accessed: 10.12.2021].

## *'Soft Targets' Protection Awareness: A Case for Specialized Security Education Need*

### *Abstract*

Education for security is a very broad concept. It is also often associated with a strategic understanding of security. Meanwhile, its importance is also visible in much narrower areas concerning selected security categories. This article aims to indicate the relationship between education for security and the issue of protecting 'soft targets': defenseless, unsuspecting civilians who become targets of terrorist attacks. Moreover, the article identifies the principles of soft targets protection.

**Key words:** soft targets, terrorist attacks, education for security, protection rules

### *Świadomość ochrony „miękkich celów” – przykład potrzeby specjalistycznej edukacji w zakresie bezpieczeństwa* *Streszczenie*

Edukacja dla bezpieczeństwa to bardzo szerokie pojęcie, ważne także w znacznie węższych obszarach dotyczących wybranych kategorii bezpieczeństwa. Celem artykułu jest wskazanie związku między edukacją dla bezpieczeństwa a ochroną tzw. miękkich celów, czyli cywili, funkcjonujących w przestrzeni publicznej, którzy stają się celem ataków terrorystycznych; omówiono również zasady ich ochrony przed takimi zagrożeniami.

**Słowa kluczowe:** miękkie cele, ataki terrorystyczne, edukacja dla bezpieczeństwa, zasady ochrony

### *Schutzbewusstsein 'weicher Ziele': Ein Fall für den Bedarf an spezialisierter Bildung für Sicherheit* *Zusammenfassung*

Bildung für Sicherheit ist ein sehr breites Konzept. Es wird auch oft mit einem strategischen Verständnis von Sicherheit in Verbindung gebracht. Ihre Bedeutung wird mittlerweile auch in sehr viel engeren Bereichen bei ausgewählten Sicherheitskategorien sichtbar. Dieser Artikel soll den Zusammenhang zwischen der Bildung für Sicherheit und dem Schutz „weicher Ziele“ aufzeigen: wehrlose Zivilisten, die Ziel von Terroranschlägen werden. Darüber hinaus identifiziert der Artikel die Prinzipien des Schutzes von weichen Zielen.

**Schlüsselwörter:** weiche Ziele, Terroranschläge, Bildung für Sicherheit, Schutzregeln

### *Понимание необходимости защиты «мягких целей» – пример профильного образования в области безопасности* *Резюме*

Профильное образование в области безопасности – это очень широкое понятие, которое затрагивает также более узкие вопросы, касающиеся выбранных категорий безопасности. Цель статьи – показать взаимосвязь между образованием в области безопасности и защитой так называемых «мягких целей», то есть гражданских лиц в общественном пространстве, которые становятся объектами террористических атак. В статье обсуждаются также принципы защиты гражданских от таких угроз.

**Ключевые слова:** «мягкие цели», террористические атаки, образование в области безопасности, принципы защиты

