SHIELD

solutionS to enHance Interfaith protEction of pLaces of worship from terrorist Danger

This project was funded by the European Union's Internal Security Fund — Police under grant agreement No. 101034229.

PROTECTING PLACES OF WORSHIP FROM VIOLENCE AND TERRORIST DANGER: A QUICK GUIDE FOR LOCAL STAKEHOLDERS AND PRACTITIONERS

Edited by Luca Guglielminetti and Alessandro Marani

CREDITS
Reviewer: **Francine Martin (SYNYO) and Cristina Gillio (CIRS)**
Graphic Design: **Andrea Ceccaroni (Spin System)**

This handbook is in the framework of the SHIELD project, funded by the European Union's Internal Security Fund — Police under **grant agreement No. 101034229**.

DISCLAIMER: The content of this handbook represents the views of the authors only and their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

TABLE OF CONTENTS

01 INTRODUCTION

This handbook is a concise and smart guide on the main outcomes and recommendations of the SHIELD project **to support the protection of places of worship from terrorist danger**. Behind the SHIELD project there is a consortium of 18 partners from 10 EU countries, working from January 2022 to March 2024, and funded by the European Union's Internal Security Fund in the framework of its Counter-Terrorism policies and action plan. Such a plan has the aim to support the protection of public spaces, to develop better capacities to detect and mitigate threats, to improve the resilience of communities as well as raising citizens' awareness, and engaging more at regional and local level, as well as at international level.

SHIELD's analysis was focused on a subset of public spaces: the places of worship that intrinsically possess a special value that has to be carefully preserved. In fact, both believers and non-believers of all communities recognize them as having with a strong symbolic value around which the common sense of identity feeds the social cohesion at the local, national and European level.

The project consortium, involving a wide range of stakeholders and experts on the topic, has developed a set of strategies, tools and recommendations that we now share with the readers of this handbook, which is intended **for the leaders of religious communities, their security managers, local policy makers and LEAs representatives**. **The aim** is to provide **information and practical** guidance that can support a comprehensive protection system.

In particular:

1

On the one hand, **to raise awareness**:

- on the issue of security based on our analysis of the data and trends of violent or terrorist attacks on places of worship in Europe in the last two decades, for each of the three main religions: **Christian, Jewish and Muslim**;
- on the prevention practices and approaches to violent radicalisation and polarization.

2

On the other hand, **to provide practical and operational guidance**:

- on risk **assessment tools** for the identification of the most vulnerable parts and events in places of worship;
- on the technical **security measures** to be implemented to enhance the interfaith protection of places of worship;
- on mitigation approaches in the aftermath of an attack by following emergency protocols along with the provision of support services to the victims.

To make the most of the contents of this handbook, our preliminary recommendation to the readers is to bear in mind the importance of establishing and maintaining cooperation between public authorities, religious leaders and security experts, which includes creating clear communication channels and providing information and awareness on security threats.

In order to facilitate the reading of this handbook, we have tried to reduce specialist terminology to a minimum. However, a terminological clarification is necessary to conclude this introduction. It should be noted that there is no official and universally accepted definition of terrorism and that labelling a violent event as a terrorist attack entails ideological and political implications. Therefore, the SHIELD consortium has decided to adopt the broader term of 'violent or terrorist attack' to encompass all the violent offences motivated by political, religious or cultural reasons - usually referred to as terrorism, violent extremism, fundamentalisms, hate crimes - against places of worship.

Finally, the editors and reviewers of this handbook thank all project consortium partners who worked on SHIELD's analyses and deliverables. A network of religious organizations, security experts, police, city councils and technology companies who have individuals' freedom and security at heart and want communities to practise their faith and live their lives without fear.

December 2023

To ensure the widest dissemination of this handbook, the project partners agreed to provide a digital version translated into their respective national languages. They are available here: ***https://shieldproject.eu/handbook***

SHIELD
Solutions to enHance Interfaith protEction of pLaces of worship from terrorist Danger
SHIELD

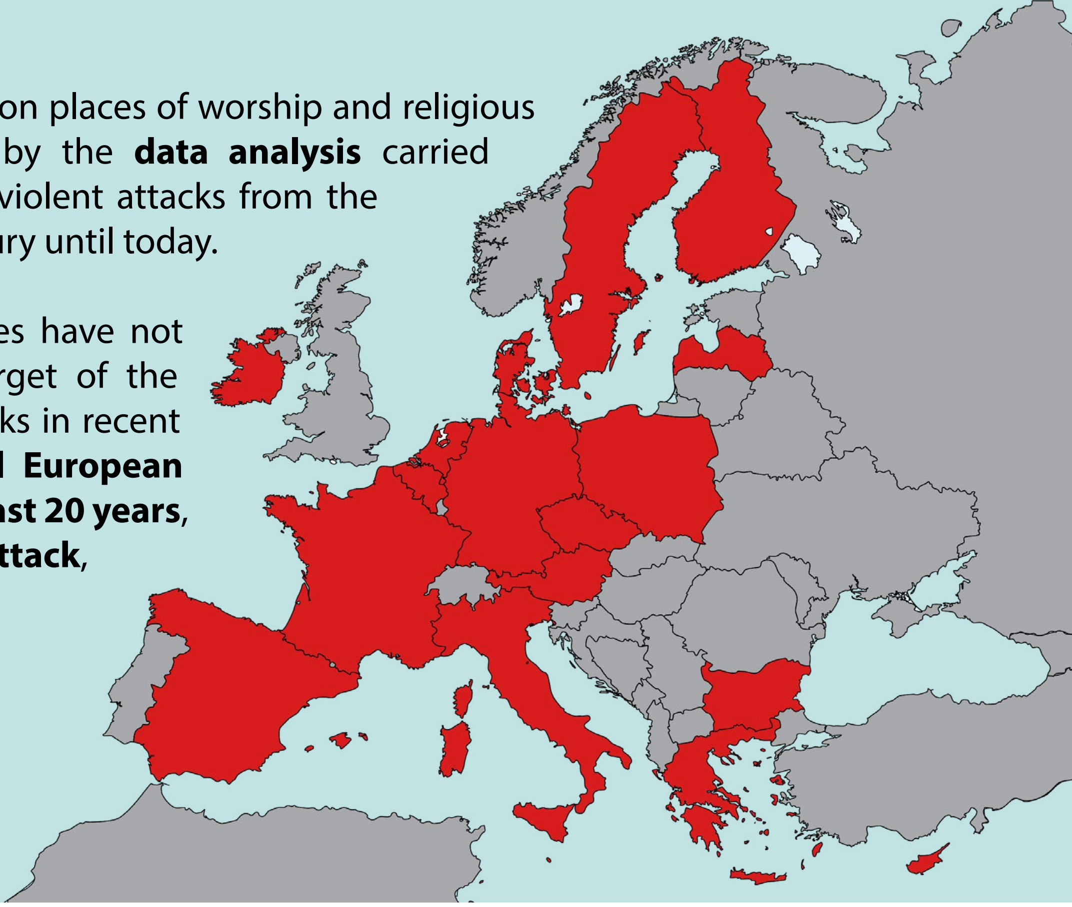
The Shield project first workshop on the 1st December 2022 at the 'Grande Moschea' of Rome

02

STATISTICS DATA ANALYSIS

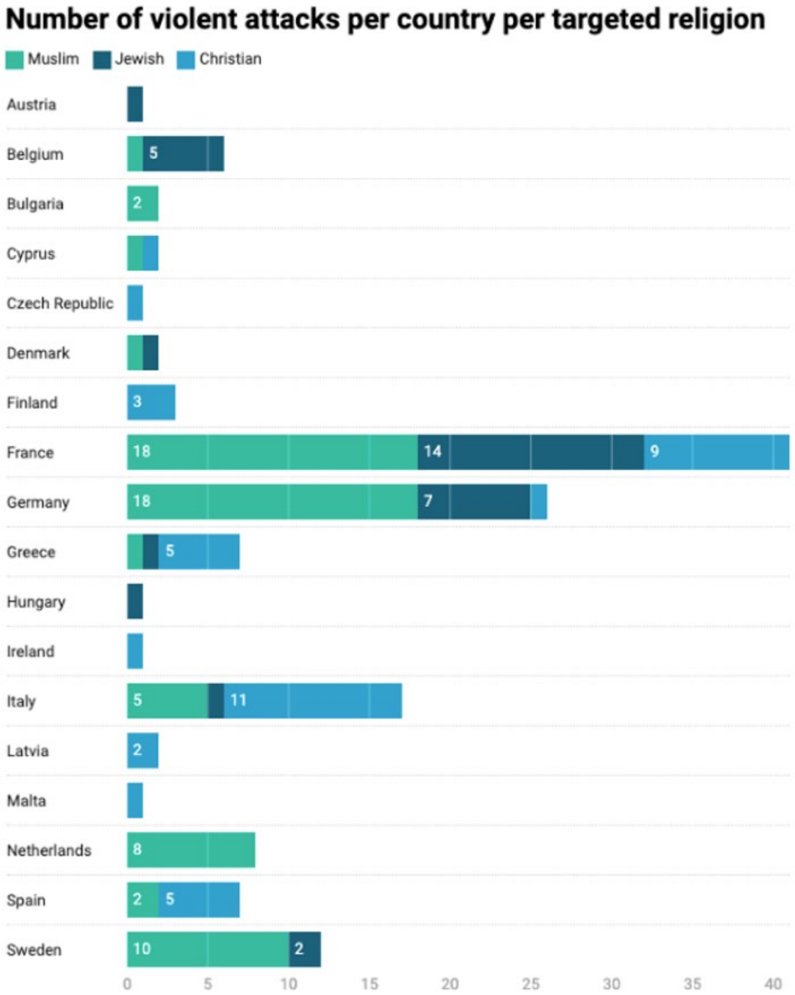
The relevance of the focus on places of worship and religious buildings was confirmed by the **data analysis** carried out by SHIELD project on violent attacks from the beginning of the 21st century until today.

In fact, even if these places have not always been the main target of the most serious terrorist attacks in recent years, however, almost **all European countries have, over the last 20 years, suffered a direct violent attack**, as shown in the picture.



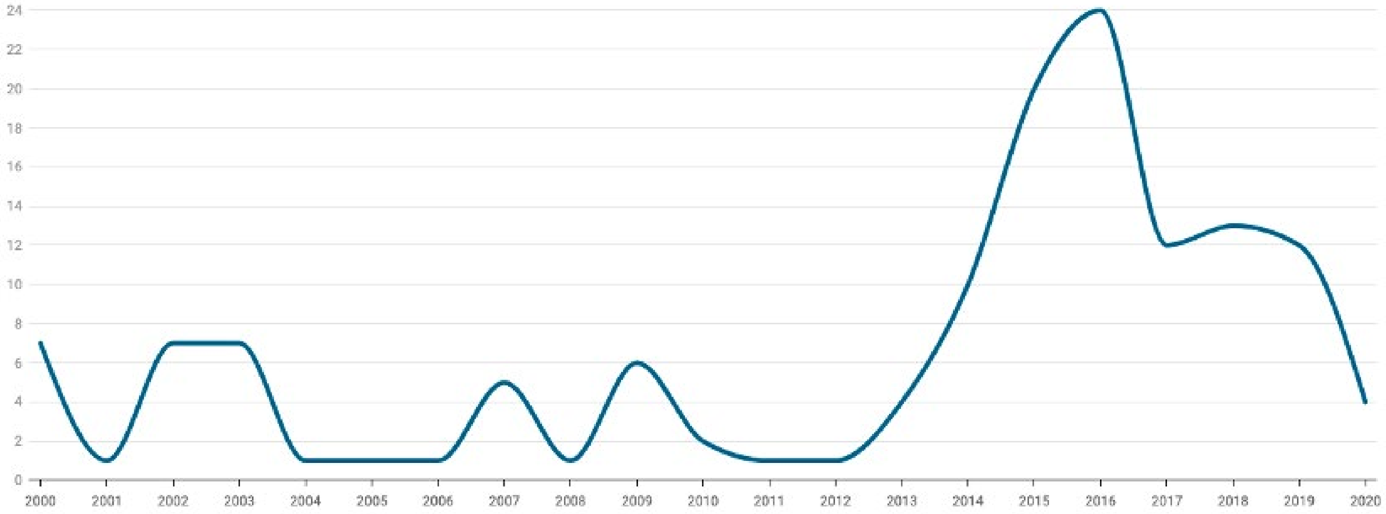
EU Countries that have experienced at least one violent attack on religious buildings

Based on the same data collected analysis, the SHIELD project also reported the distribution of violent attacks by targeted country and religion, focusing on the three main monotheist faiths, as highlighted in the graph below.



Number of violent attacks per country per targeted religion

The following table illustrates the quantitative distribution of the attacks on the timeline, showing clearly the fluctuation wave along the last 20 years and the peak between 2013 and 2017. A peak that reinforces the motivation behind the SHIELD project to focus on the protection of religious places of worship.



Number of violent attacks on places of worship between 2000 and 2020

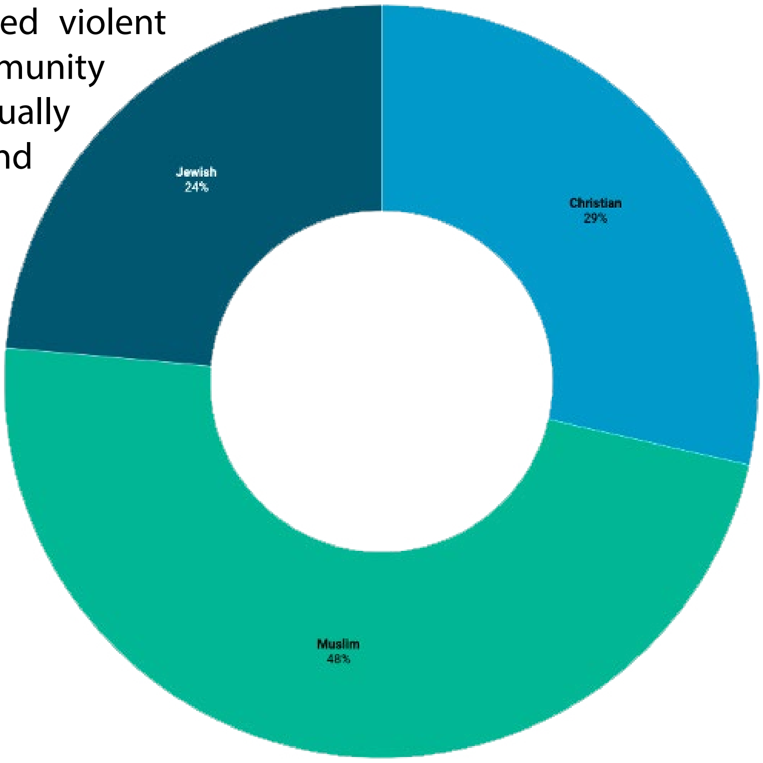
Furthermore, almost half of the recorded violent attacks were against the Muslim community (48%), while the rest of the attacks are equally divided between the Christian (29%) and Jewish (24%) communities.

Percentage of violent attack toward the 3 monotheisms in the EU

🟦 ***Christian***

🟩 ***Muslim***

🟦 ***Jewish***



This statistical data, that include the attacks on both buildings and people, allows to draw some **rather relevant considerations**:

1. **Muslim community**: it often targeted by attacks in countries with larger Muslim communities, such as France, Germany, and Sweden. However, Italy and Holland have also experienced significant attacks despite having a low percentage of Muslims. Political-religious conflicts have contributed to a rise in white supremacist violence and right-wing extremism, resulting in numerous acts of terrorism against Muslim places of worship.

2. **Christian community**: it faces various types of attacks that are difficult to analyse, as they have different motivations and actors behind them. Some of the attacks are motivated by vandalism (as for other communities), extreme left-wing or anarchist groups (especially in Greece and Italy), and mainly Islamic jihadism, which aims to destroy and undermine symbols of European identity, and sometimes to harm people directly.

3. **Jewish communit**y: it suffers from surprisingly violent attacks, which often result in casualties. Although they represent only 25% of the total attacks, and only 0.2% of the entire population of the European Union, they are disproportionately targeted by a range of actors, especially the extreme right and jihadist Islam.

This data analysis, besides offering a picture of the European situation over the two decades, served as a basis for the SHIELD Project to examine the modus operandi present in all these attacks. Through this examination and the additional twenty interviews conducted with representatives of the various religious communities, we were able to:

a. assess the level of awareness and preparedness of the different religious communities in Europe and thus;

b. develop the proposed vulnerability assessment tool and the appropriate security measures, adapted to the possible scenarios based on the type of religious building and its location, presented in chapters 4 and 5 of this handbook.

03

EARLY PREVENTION

The analysis of the recent attacks presented in the previous chapter, revealed that the religious places were not adequately protected due to an underestimation of the risks. In fact, despite the risk was identified at a national level, **small and/or local places of worship were either unaware of the risks or unable to implement mitigation measures**. Therefore, before presenting the vulnerability assessment and the security measures, it is important to recommend some **approaches and practices to raise awareness** at an early stage of prevention.

A lack of perception of the risks at the local level may denote a lack of awareness on how political violence works: **a geo-political event, far from our communities, can cause repercussions and affect them**. We have a striking example of this dynamic in the Middle East war which broke out on 7th October 2023 and which immediately led to a resurgence of terrorist attacks in Europe in the following weeks; a global rise in incidents of anti-Semitism and Islamophobia; and a related growing alarm from various intelligence or counter-terrorism agencies for the security of religious communities and places. So, since the bombing attacks in Madrid in 2004 and in London in 2005, many European countries and the European Union have developed **programs and policies to prevent radicalisation leading to terrorism**. The aim of such policies is **to increase the resilience and the efforts of local communities to interrupt**, as soon as possible, **the violent radicalisation process** before an individual or a group engages in criminal activities.

Although the SHIELD project has not been focused on early prevention work, on it has highlighted, during all the public events that has organized or attended, **the importance for local authorities, civil society and religious organisations to carry out practices that support the safeguard of the social cohesion and the resilience** of citizens and communities. Early prevention work is primarily aimed at **avoiding the risks of polarisation and radicalisation** of opinions and viewpoints on sensitive issues, irrespective of whether these are of a political or religious nature.

Interreligious and intercultural dialogue activities are the central axis of a prevention work that should always be open and continuous in a context of conflicts increasingly interconnected at the international level, as agreed by all the main religions representatives who attended the SHIELD Workshop in Rome in 2022.

The recommendation for religious communities' leaders, policymakers and LEAs representatives is therefore **to establish local networks** - open to the

relevant stakeholders such as education system, social care services, prison and probation, civil society organisations, etc. - with awareness of the risks that stem from global conflicts and with operational capacity for continuous prevention intervention **on the ground and over time**.

On the issue of polarisation and radicalisation prevention, a large **repository of practices**, that can inspire the readers of this handbook, has been developed by the Radicalisation Awareness Network (RAN), set up by the EU Commission in 2011, and available here:

RAN Collection of inspiring practices.
The RAN Collection offers practitioners, policymakers and researchers the opportunity to draw inspiration from existing practices and to find examples adaptable to their local/specific context.
https://home-affairs.ec.europa.eu/system/files/2021-05/ran_collection-approaches_and_practices_en.pdf

04

THE VULNERABILITY ASSESSMENT TOOL

In its effort to support local and regional authorities in the protection of urban spaces, the European Union's Directorate General for Migration and Home Affairs (DG HOME) has developed the EU Vulnerability Assessment Tool (VAT) or Checklist (VAC). A tool which main objective is to provide **practical support to be able to adopt appropriate measures to prevent and mitigate terrorist attacks and their consequences**.

This VAC, originally addressed to local and regional authorities, has been modified and simplified by the SHIELD project team, to meet the specific needs of places of worship. In any case, using **this tool requires good skills in the security of public space and risk management**, so we recommend the readers of this handbook to create **a small multi-agency team** involving the proper skilled experts.
The local security policy should always contain a reference to the mitigation of the risks that are critical or serious to the targeted asset, in our case the places of worship. **The VAC is an objective and rational way for stakeholders to set their action plans and the technical security measures, as described in the following chapter**.

The SHIELD VAC follows the idea that general risk is the multiplication of three factors:

1. Sensitivity of the site (based on size, usage, architecture)
2. Threat to the site (by *modus operandis* and by security zone)
3. Protection measures (by layers of security) to decrease/mitigate the risk

The threat is highly dependent on the local parameters of damage and likelihood that are shown in a matrix table to be set by experts by each site.

In order to obtain the results of the risk assessment for each space or building, the list of factors analysed within the VAC needs to be inserted in the matrix table which is part of the **online directory** along with **all the relevant files**.

The VAC files - which includes: **a)** the methodology explanation, **b)** the VAC and **c)** the Excel (matrix) to obtain the assessment – are available here: ***https://shieldproject.eu/handbook***

05

TECHNICAL SECURITY MEASURES

Security: A Matter for All Religious Communities

In the European Union, the approach to the protection of religious communities varies somewhat from country to country. In some Member States, the protection of religious communities is seen as a responsibility of the government and is supported by both law enforcement and financial means. In many Member States, however, religious communities do not have State support and must therefore mitigate the risks they face using their own resources. The costs of building and operating security systems are very high, so it would be worthwhile for the European Commission to discuss this issue thoroughly.

The SHIELD project findings highlight that the fundamental goal of these security measures lies in safeguarding human life as the foremost priority. It is imperative for religious communities to prioritize ensuring the safety and freedom for individuals to live their lives and practice their faith without fear. Thus, the security measures primarily focus on preventing attacks that endanger human lives rather than solely protecting property. While safeguarding property remains essential, it is secondary **to preserving human life**. The deployment of security systems involves **a layered approach**, wherein individual solutions function independently. Ideally, multiple security measures operating simultaneously aim to counter a potential attack effectively.

Religious communities, local authorities and LEAs in Europe should consider some **security principles** which are the following:

1. **The purpose of defence is to protect human life.**
   The protection of property is important, but not as important as the protection of the safety of community members, guests, and visitors. It is not acceptable that the life or way of life of the community should be endangered.

2. **Preventing attacks is more effective than defeating them.**
   Preparation is needed to ensure that the community is able to respond to specific threats and attacks, but the focus should be on preventative methods first and foremost. Prevention encompasses many things, from passive means of protection, to creating protection plans and processes, to being well trained to respond.

3. **The security system must be systematic and layered.**
   Attacks should be kept as far away as possible from the sensitive area. Progressively stronger barriers and controls should be placed between the people being protected and the attackers, which should be able to operate independently of each other.

4. **Resources should be shared proportionally between the three pillars of defence.**
   Technologies, human resources and procedures will only work effectively if they are developed in equal measure. The results of continuous risk analysis should be taken into account in the development of the pillars of defence. In the event of new risks, the necessary responses must be found, taking into consideration that this must be based on the cooperation of technology, human resources and security processes.

5. **In their operations, defence forces must be proactive rather than passive in their operational processes.**
   Active patrols, checks and vigilance tests are necessary. These ensure both the necessary deterrent effect, prevention and high quality. Maintaining dynamic defences is not an easy task, especially in the case of prolonged periods of no or no detected hostile operations.

6. **Training and drills for both security personnel and the community must be continuously ensured.**
   It is not enough to acquire only theoretical knowledge; security drills must be conducted regularly. Simulations should be carried out, including the involvement of crisis management.

7

Systematic but random verifications and audits of the functioning of security systems should be carried out.

All technologies and standards are only as strong as the compliance with them. Wherever possible, the operation of security systems should be measured and evaluated (tactical exercises, self-audits, staff surveys) to demonstrate improvements in quality.

8

Ensure that adequate staff are in place to carry out security duties.

The person responsible for security should be directly accountable to the community leader but should also have considerable responsibility in his/her own area, with the appropriate authority. Reliable and highly skilled professionals should be selected who are committed and professionally competent.

9

Good relations must be established and maintained with the designated professionals within the Authorities.

In line with the principle of prevention, information about suspicious events should be shared and warnings should be taken into account. It should be made clear to the authority's designated contacts that their views and involvement are important for the security of the community, and that incidents detected and shared by the community will help to prevent crime.

External fences

"A physical barrier is a mean of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a building and can help to restrict, channel or impede access and constitute a continuous obstacle around the site. Physical barriers can create a psychological deterrent for anyone planning an unauthorized entry. A number of elements may be used to create a physical barrier, some natural and some manmade. Natural barrier elements include rivers, lakes, waterways, steep terrain and other terrain features that are difficult to traverse. Manmade elements include fencing, walls, bollards, planters, concrete barriers".

Fences and walls are the most common form of protection of all places from unwelcome intrusion. In addition to their primary security function, fences and walls demarcate the space of a place of worship and in particular its outer perimeter. Fences can be of many types with different technical characteristics, from those that are purely delimiting and aesthetic, to those capable of stopping even heavy vehicles thrown at them at great speed.

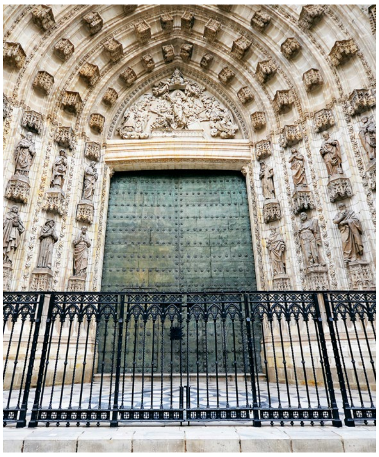
Fences are very effective, as they form both a physical and psychological barrier that delimits a well-defined area. Fences, however, have some fairly precise limits: if they are too low and/or made of non-resistant material, they cannot be effective because they are subject to degradation, break, and cannot withstand a vehicle or an explosion. Moreover, they can easily be bypassed, defeating their function.

Another element to consider is the surveillance of the fences: without a minimum of surveillance equipment (CCTVs), one risks relying on the perception that the fences will not be climbed over. Fences are then absolutely unable to stop armed individuals. Nevertheless, they are often indispensable tools when securing a place of worship, as they form an initial barrier, a boundary, between an external perimeter and the place of worship.

Finally, it should be remembered that fences should be designed with the right balance between the need for security and cohesion with the surroundings, while also respecting local regulations on the installation of security barriers.

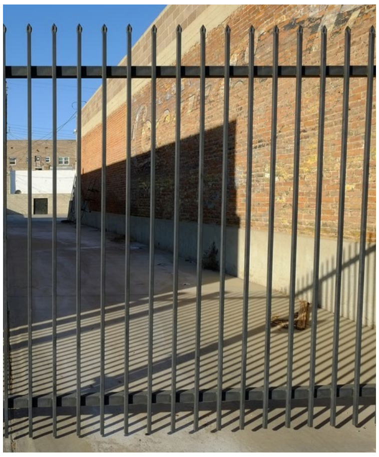
As it can be imagined, the most critical feature of the fences is, apart from the likelihood of the peripheral boundary being breached without adequate control, the entry point, which if unguarded, is a key critical point.

There are many types of fences, here is a non-exhaustive list of fences, depending on different characteristics:



Metal railings:

this type of fence is one of the most suitable for the security of places of worship. Aesthetically, they can be adapted to any context, because if built new, they can echo the style of the place of worship or the surrounding buildings. Material-wise, they are usually made of wrought iron, which makes them very safe and durable, although they do require maintenance. Their cost is higher, but they usually do not allow them to be climbed over, they resist vehicles breaking through, and if accompanied by metal sheets they also offer good privacy.

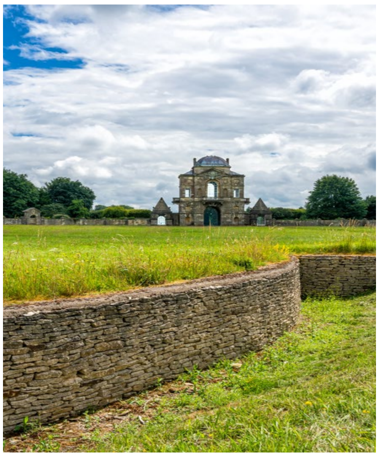


Vertical bar fencing/steel fencing:

this type of fence is a good compromise between cost and effectiveness. Steel fencing can also be created in such a way that it cannot be scaled and is of various heights, even up to 4 metres. Depending on the thickness and type of metal used, they can also be able to stop vehicles from breaking through, especially if there is reinforced concrete at the base of the perimeter. This type of fence is also aesthetically more adaptable to various contexts.

Welded mesh fencing and/or chain link:

this type of barrier is by far the cheapest, the easiest to install and with very little maintenance costs. It is available in various heights, but the most common is around 1.80 metres. Although it is the easiest and cheapest fence, it is also the one that offers the least protection, as it can easily be climbed over and damaged, is not at all resistant to vehicles breaking through, and aesthetically may not enhance the place of worship. Only if the fence is fixed on a reinforced concrete base around the perimeter, then it could stop vehicles, but, in any case, all existing vulnerabilities remain.



Ha-ha barriers or 'saut de loup' barriers:

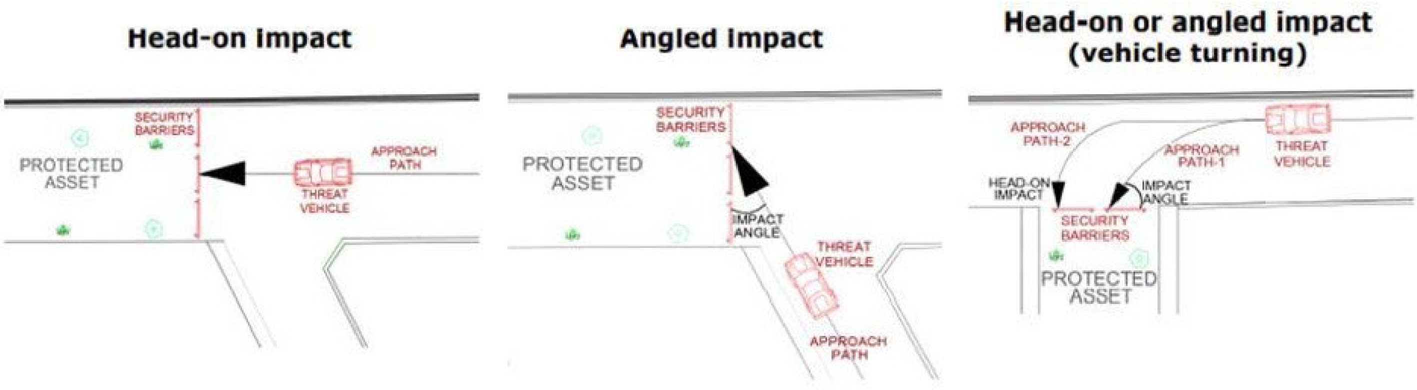
ha-ha barrier is a recessed landscape design element that creates a vertical barrier (particularly on one side) while preserving an uninterrupted view of the landscape beyond from the other side. It prevents vehicles and unauthorized people to enter a determined area while keeping the view from the inside to the exterior.

Anti-ramming systems

In recent years there has been an increasing trend in vehicle ramming attacks against soft targets as people. This growing tendency of vehicle attacks, characterised by the ramming vehicles that are either deliberately driven at high speed against the public to maximise human casualties or are used for transporting an improvised explosive device (IED) close to a facility, concerns also places of worship.

The increased use of vehicle attacks is attributed to their relatively easy planning, accessibility and minimal expertise required in carrying out the attack. In order to block or minimise the damages of these attacks an effective strategy for the protection of physical perimeter is required. This strategy is based on the implementation of anti-ramming systems, which are obstacles acting as a barrier. These anti-ramming systems stop an ill-intentioned vehicle if it attempts to breach the security perimeter by forcing it to reduce speed or stop completely, disabling it before causing destruction and injuring people. These systems should be placed across roadways and passages and can be active or passive, permanent or temporary and can be made from various materials, such as steel, concrete and rock. Large plants and trees could be also used as anti-ramming systems, and they are less impactful (but nevertheless with the same degree of effectiveness) and more environmentally friendly with regards to the surroundings.

In order to understand which the most efficient anti-ramming systems are for a specific religious site, a risk and vulnerability assessment should be carried out, in particular by imagining multiple scenarios of attack, the potential size and speed of the vehicle, the possible attack routes. These elements will help in determining the type of barriers needed.



Example of scenario and trajectories calculation

The goal of the barrier is to absorb the kinetic energy of the speeding vehicle at the point of impact, halting its penetration or causing it a significant damage so that it will need to stop very shortly afterwards. Additionally, these barriers may act as a deterrence factor, functioning as a psychological obstacle against potential attackers.

Below we have added some examples of anti-ramming systems or other architectural elements that could be used as anti-ramming systems:

Bollards:

these elements are one of the most commonly used form of barrier. They are predominantly used in city centres and pedestrian areas. Normally made of steel, reinforced concrete or a combination of these two materials. Their narrow form and small size make them less intrusive in comparison to other solutions. Bollards are a cost effective and pragmatic solution that could be largely employed for the protection of places of worship. Bollards could be fixed or retractable, and equipped with lights if they need to be visible.

Temporary barriers:

they are re-deployable, and because they aren't built with a foundation on the ground, they rely on the aggregation of multiple barriers in order to prevent ramming attacks. They are usually used during large public events, or as temporary installation in order not to intervene on the ground, even if sometimes this temporary solution became the perennial solution. Unfortunately, these elements are not the most efficient in order to protect houses of worship and they do not fit very well with an urban landscape. They are helpful in the case of a large public event attracting crowds but not as a long-term solution.

Landscaping and architectural elements:

hardened street furniture and streetscape element which smoothly integrate and blend into the urban setting are also used a valuable form of barrier in order to block vehicle attacks. They consist sometimes of dual or multiple use elements (such as lampposts, bus stops, signposts, sculptures, benches) and their main added value is their minimal visual impact. When they are combined with other form of barriers like bollards, they become very effective. Below there is a partial list of potential elements that could be used as anti-ramming systems:

Benches in reinforced concrete:

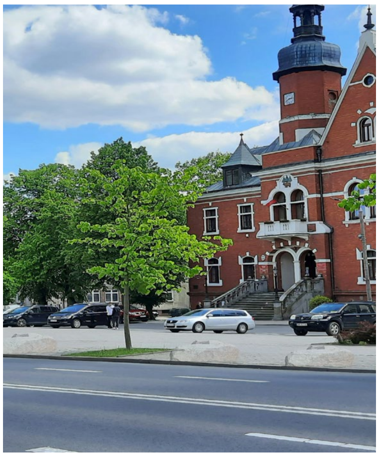
this element could be an excellent form of protection, if positioned in tactical and precise positions. They could be positioned in order to create a fictive perimeter around the PoW or in pedestrian areas in order to avoid vehicle approaching. Also, they could be well integrated with the environment by covering the bench with wood and decorative elements as plants. It is important to keep in mind that the structure should be somehow built in the ground in order to avoid fragmentation in the case of an explosion. Another element that could be considered is a wall in concrete, which is very effective but unfortunately doesn't always aesthetically fit with the surrounding environment.

Large pots and flowerbeds:

they could be made of metal or better if of reinforced concrete and should have the same characteristics of the aforementioned benches, in particular the material chosen should be a potential threat to life causing injuries in the case of an explosion. The same approach is valid for earthen hills with plants, concrete benches interspersed with plants and/or grass.

Trees:

large trees are a very valid source of protection against the tentative of a vehicle penetrating a perimeter, especially if trees and placed in a dense row. Obviously, the trees should be quite big and large and maybe they are not suitable for a city centre old town, but they could be a valid option for PoW surrounded by big empty spaces. Trees have not only a great landscaping value, but also a protection effect. For example, in case of an explosion, trees could, on one hand, restraint the blast, but on the other, be a source of potentially serious injuries. Rows of tress could be considered also an integrative element of a fence, so they will be only briefly mentioned in the section dedicated to fences.



Boulders and rocks:

when their size is especially big and if densely placed they can act as barrier in order to prevent a vehicle forcing the perimeter. Depending on the type of mineral they could be resistant at different degree to an explosion.

Planting hedges:

Planting hedges can be a good alternative to building a perimeter wall for security purposes, especially for places of worship or other public places. It can help obstruct the view of potential attackers and make the area more natural, while also being cost-effective. However, it's important to choose the right type of vegetation for the specific climate and location where they will be planted. The wrong type of plants may not provide enough cover or may require excessive maintenance, which can negate the benefits of using hedges for security. Additionally, some types of masts can provide protection against shock waves caused by explosions. Therefore, it's important to consider the specific security needs of the area when choosing what type of vegetation and other natural defences to use. Overall, planting hedges and other forms of natural defence can be an effective way to enhance security while also maintaining the natural beauty of the area. However, it's important to carefully consider the specific needs of the location and choose the right type of vegetation and other natural defences to ensure they provide the necessary protection.

Security personnel

Among the many existing solutions for the protection of places of worship (PoW), that of security personnel plays a very important part. There are mainly three types of patrolling possible:

1. Foot patrol;
2. Motorised patrol;
3. Hybrid patrolling (the patrolling is performed by unmanned vehicles which could be remotely followed by humans).

Obviously, the fundamental element to take into account when choosing one of the two solutions is the geographical extent of the territory to be patrolled and the costs of resources to be involved in.

French soldiers patrolling

It should be reminded that patrols and identifiable security personnel are by themselves a form of deterrence. Nevertheless, the objectives of security personnel are to ensure the security of determined zones, in particular:

- the surroundings of the PoW, including parking areas, pavements, and access roads;
- the immediate exterior of a PoW;
- the interior of a PoW;
- other elements (buildings, equipment, materials) that could be a threat for the safety of people or for the security of buildings.

Among the duties of security personnel, it should be mentioned the constant verification of already identified weak spots; the checking of entrances; the verification of the status of security barriers (fences, locked doors, gates etc.) and suspect behaviour of people and the identification of potential threats as object left unattended.

If patrolling is not guaranteed from LEAs and instead is organised by religious communities themselves, some basic principles should be followed. By applying these measures, some security gaps could be avoided:

- **Patrolling should be unpredictable**: different timing for patrolling should be arranged in relation to the needs of the PoW and to the specific situation (e.g. if the PoW is open throughout the week, if it is always crowded, what are the events that attract lot of people). The frequency and timing of patrolling should be determined following an appropriate risk and vulnerability assessment.
- **Patrolling routes should not be always the same**: it should be taken into consideration the creation of different roadmaps for patrolling. If the surrounding area has small roads (e.g. city centre of an old town) consider at least different starting and ending points.
- Patrolling consists not only in physical presence as deterrence, but also in daily specific activities as the verification of the following elements:
  - » the conditions of infrastructures and security elements (barriers, fences, and effective restriction of locked areas, etc);
  - » punctual verification before and after specific events where crowds are expected;
  - » suspect behaviour of people in the surrounding areas;
  - » suspect circulation or parking of vehicles;
  - » vandalism acts, especially if hate speech is spread;
  - » the integrity of the security infrastructures after violent natural events.

Video surveillance

Systems for video surveillance are very helpful for allowing quicker intervention from emergency responders and for detecting unusual behaviours, such as potential spying activities. To accomplish such an objective, it is essential that they are continuously monitored by an operator. Systems that only record data and do not transmit images in real time are significantly less effective because they only allow for the probation of facts during the trial. But, in areas with very little risk, these solutions may also be considered. The national legislation, which might vary greatly depending on the country, must always be checked and consulted when it is matter to protect privacy. Solutions for public- private collaboration and integrated security can be explored in various nations. These options call for the installation of a video camera, which the private body pays for but which sends images to the police operating room. The cameras can then be pointed at an open public space.

Because cameras can be fitted with sensors that can detect potential intrusions, intrusion alarm systems were not taken into consideration in this analysis from a cost-saving perspective. Of course, the end user is free to install intrusion detection systems as well for increased security.

Security cameras are fundamental and now almost ubiquitous elements in many houses of worship. They can be divided into many types, but first of all two essential distinctions must be made:

- **Cameras that record but do not send images in real time to a control room**: these cameras are certainly useful as a psychological deterrent but have no preventive element. Since they are not connected to a control room, there is no operator able to monitor the situation in real time and/or intervene in the event of an alert. This type of camera is only useful in cases of low risk and where security risks are only related to property such as attempted intrusions for theft and vandalism.
- **Cameras with connection to a local control room or monitoring room**: this type is the most suitable for effective prevention and to thwart the most serious threats directed against people. In this regard, an important element to stress is the role of the monitoring operator(s), whose duty is to monitor any potential threats. CCTV systems should be tailored to the needs of PoW after having conducted a risk and vulnerability assessment. There are two main elements to consider while talking about CCTVs:

  1. Type of cameras;
  2. Location of cameras.

1. TYPES OF CAMERAS

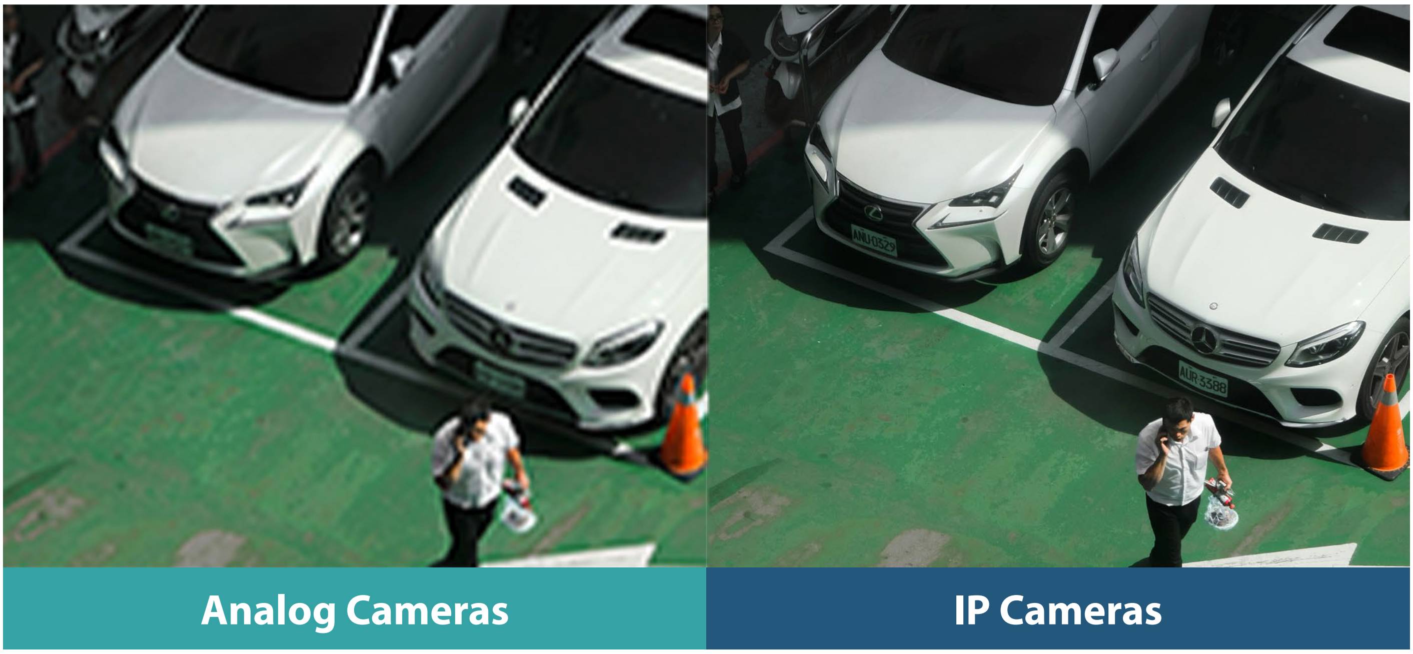
There are two main types of cameras:

1. Digital cameras (or IP cameras)
2. Analogue cameras

Internet Protocol (IP) cameras are all those digital cameras capable of sending and receiving data via an IP network. They are widely used as video surveillance cameras and come in different designs and capacities. Analog video cameras, on the other hand, capture images, record them and send them as analogue signals via a coaxial cable to a digital video recorder (DVR). The latter then converts the analogue signals into digital signals, compressing the file and storing it on a hard disk.

Before highlighting the main differences, pros and cons of analogue and IP surveillance cameras, several factors are often overlooked when making comparisons between the two types. These include two main elements:

1. resolution: IP cameras capture better quality images with a higher resolution and have a much wider field of view than analogue cameras;
2. storage: an IP camera can consume up to 6 times the disk space of an analogue camera in the same amount of time. This also depends on the resolution and HD specifications of the cameras.



Analog Cameras

IP Cameras

PRO AND CONS OF IP CAMERAS

Pro	*Cons*
IP cameras have several sensors in one device and can cover a wide angle of view. In addition, they have a higher resolution and thus higher quality images.	Compared to analogue cameras, IP cameras are more expensive to install. However, they are easier to customise and scale than their analogue counterparts.
As technology improves and more of these products come onto the market, IP cameras are becoming more and more affordable. Today we have several entry-level IP cameras that are worth buying.	They are high-resolution and therefore take up a lot of storage space.
IP cameras are easy to install: no encoders/decoders are required and only one cable is needed for power and data connection to a network switch.	These cameras have a user interface that may require some learning by non-tech-savvy people.
They offer increased security as the video is encrypted before transmission.	

PRO AND CONS OF ANALOGUE CAMERAS

Pro	*Cons*
They are significantly cheaper than IP cameras, especially when more cameras need to be installed.	Analogue security cameras are not ideal for areas with a lot of movement, due to their low frame rate and image quality.
Analogue cameras are easy to use and do not require a learning curve.	They occupy less space, so more analogue cameras are needed for a given project than IP cameras.
High-definition (HD) analogue cameras are now available on the market and have significantly improved image and video quality.	They do not have data encryption technology; therefore, images and videos are susceptible to digital hackers.
It is easy to find an installer at a relatively low price.	

There are then different types of cameras, depending on their characteristics and destination:

- Indoor cameras: these cameras are specifically made for indoor areas and are normally in HD but with cheaper material than outdoor cameras.
- Outdoor cameras: the weather resistance is the primary distinction between indoor and outdoor IP cameras. The latter are made to tolerate significant variations in temperature and humidity, whereas the former is appropriate for situations with nearly constant temperature and humidity. In addition, outdoor IP cameras need to be capable of withstanding snow, rain, and dust by insulating the shell that houses the electrical circuits.
- Pan Tilt and Zoom cameras (PTZ): this camera is capable of panning horizontally (from left to right), tilting vertically (up and down), and zooming (for magnification). PTZ cameras are often positioned at guard posts where active employees may manage them using a remote camera controller. Their primary function is to monitor expansive open regions that need views in the range of 180 or 360 degrees. Depending on the camera or software being used, they may also be set up to automatically monitor motion-activated activities or adhere to a defined schedule.
- Infrared Night Vision cameras: this camera allows to maximize video surveillance effectiveness in low light conditions.
- Bullet CCTV: most bullet cameras will offer LEDs that allow the camera to see well in the dark or in low light situations; it can be used on the interior or exterior and can withstand harsh weather conditions or extreme temperatures. Bullet cameras are known for their longer range rather than their wide-angle field of view capabilities and they can be mounted on any wall, making them a great option for external monitoring.
- Dome cameras: dome security cameras are a versatile and visually subtle option for surveillance. The housing is dome shaped as the name suggests and is usually placed on ceilings or under eaves as they need a horizontal surface to be mounted on. They are extremely durable with vandal-resistant housing and can withstand all the elements both internally and externally. Most dome camera options will include smart-infrared night vision surveillance, high resolution images, and wide dynamic angle imaging to cover a wide range of areas.
- 360º CCTV: it can capture omnidirectional videos or photos.
- Cameras able to distinguish between people and animals in order to recognise potential threats and send alerts to the security operators
- Cameras with positioning systems
- Cameras for license plates recognition
- Camera able to count people

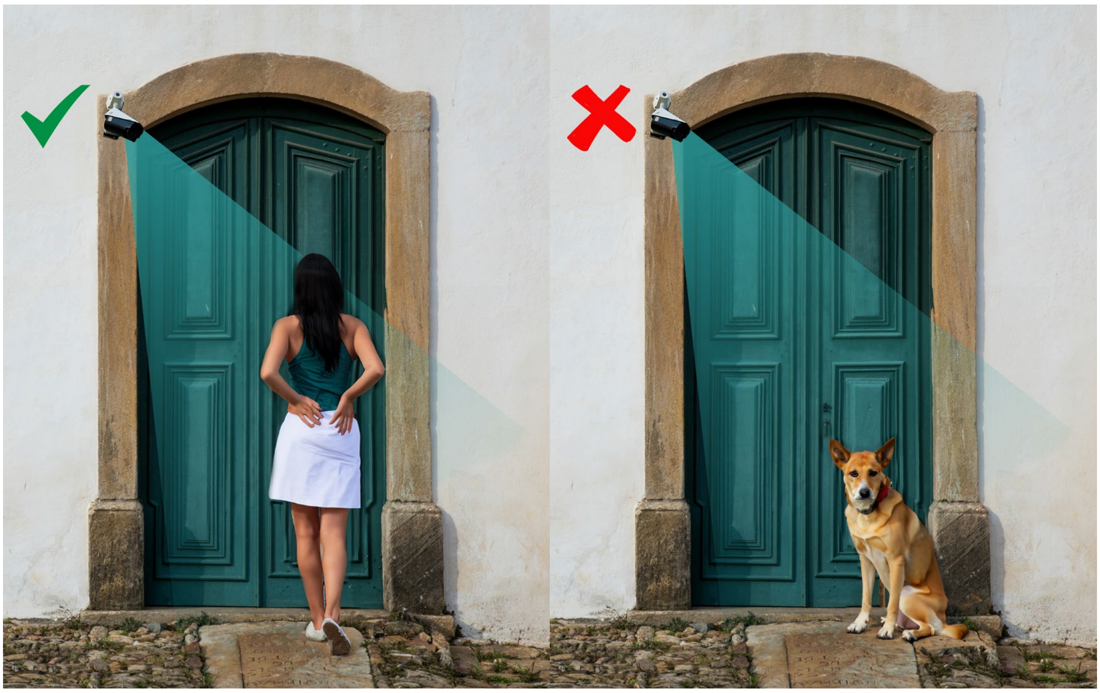
Almost all these cameras (IP cameras) could be integrated with other sensors (movement, fire, etc) in order to automatically send an alert to security personnel.

Pan Tilt and Zoom camera (PTZ)

Bullet camera

Dome camera

360° camera



Camera able to perform human recognition

2. LOCATION OF CAMERAS

In addition to having presented the different types of security cameras and their characteristics, it is also necessary to look at their possible location and other guidelines to maximize the cameras' potential.

One of the first things that comes to mind is that the placement of cameras should be carefully thought out: fewer cameras than actually needed will leave vulnerabilities that can be exploited by malicious intruders, excess cameras will cost too much, will not be as effective as they seem, and at the same time may even intimidate PoW users. Visibly placed cameras in specific locations increase the sense of security and help in psychological deterrence, whereas too many cameras can almost induce a sense of insecurity.

In general, the elements to watch out for are the followings:

- Identify precise areas to be monitored (not everything has to be monitored);
- Pay attention to the brightness of the area to be monitored (low brightness will reduce the general definition but a light source that is too close could create annoying reflections);
- Avoid blind spots such as walls, columns, protruding objects that limit the view of the camera;
- Pay attention to vegetation: trees can be serious obstacles to the view;
- Try to make the public notice the existence of surveillance cameras, on the one hand to instil security and on the other hand as a psychological deterrent. At the same time, cameras must aesthetically integrate with the rest of the building;
- Cameras should be positioned in such a way that they cannot be degraded or vandalised without other cameras noticing. Usually the principle of 'cameras watching each other' applies.

In conclusion, it can be noticed that surveillance cameras are a very effective tool, if some rules are followed and these cameras are used in an efficient and correct way.

Lighting systems

This section describes supplementary lighting powered by an alternative source to the primary one (which could be provided by the local administration if the building is on a public road). Security lighting provides a level of illumination to clearly identify persons or objects and creates a psychological deterrent to criminal activity in the area being protected. There are four general types of outside security lighting:

- continuous lighting;
- emergency lighting;
- moveable lighting;
- standby lighting.

The motion sensor light is turned on by the motion sensor. That usually means that the light will automatically turn on as soon as this sensor (also called an occupancy sensor) notices a person moving. There may also be a mechanism to turn the light on manually, but not always.
These sensors could be connected with CCTVs and could also automatically provide an alert to the control room.

Motion sensor lighting

Active and passive fire protection systems

Active protection systems are one option that may be taken into consideration, as well as passive protection systems. It can be defined “active” any equipment that takes action in the event of a fire. An intervention, which may occur with or without a man present, is necessary for active protection. This type of fire protection includes fire extinguishers, **fire extinguishing systems with hydrants or sprinklers, smoke and heat extruders, pressurization systems, and fire detection and alarm systems.**

Any actions that lessen the effects of a fire without requiring human intervention or the activation of a device are collectively referred to as passive protection systems. The spread of the fire is prevented by these measures. Hence, they are products to protect structural components, to delimit fire- resistant compartments, or simply materials with low combustibility properties as fire barriers.

It is feasible to appropriately protect houses of worship from the risk of arson that can be initiated in a variety of ways by combining active and passive protection systems. For instance, someone could break into a place of worship at night and light up the wood furnishings or could throw a Molotov cocktail bottle at the door of a PoW during the function or as the people leave. A Molotov cocktail bottle could also be thrown inside the structure after breaking a window with a stone. Because it combines protection systems that are automatically activated with others that must be manually activated by an operator, the combination of the fire protection systems illustrated below is a good option for guaranteeing the protection of the building both during the day and at night. Nonetheless, it must be remembered that fire rules might differ significantly amongst the various European Union member states. As a result, the general ideas presented here must be elaborated upon at the time of installation under the guidance of a skilled technician who is familiar with how to implement local laws. It should also be borne in mind that under local national laws churches may not be subject to fire regulations or be subject to them but with significant limits respect others. This obviously requires a high degree of flexibility in applying what is proposed below.

Sprinkler systems

Sprinkler system

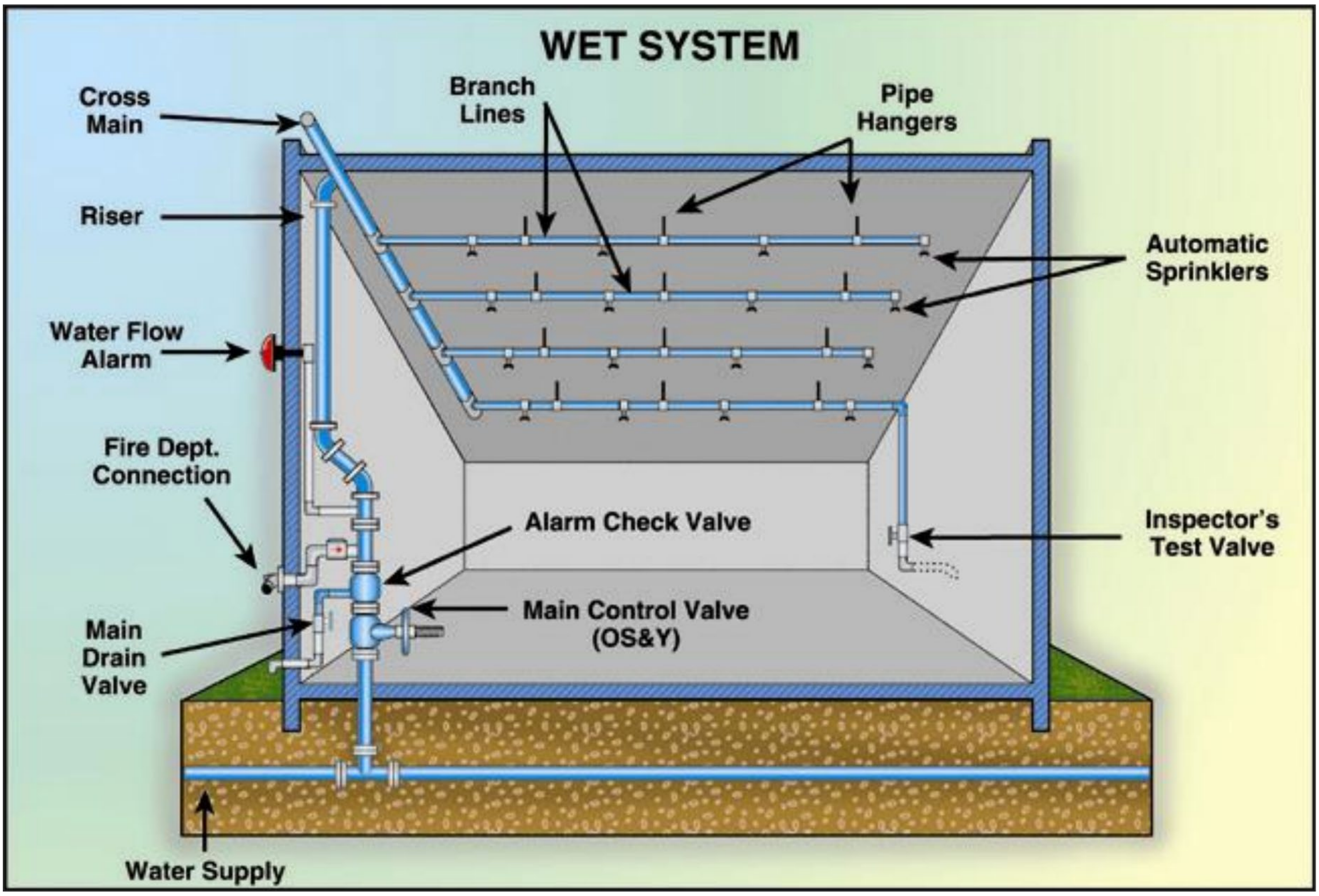
The sprinkler is an automatic rain extinguishing system. It aims to detect the presence of a fire and to control it so that the extinguishing of the same can be completed by other means, or to extinguish it in the initial stage. (ESFR - Early Suppression Fast Response).

Such a system includes one or more water supplies and one or more sprinkler systems. The system includes various sprinkler valves (the regulator is installed on the roof) and a network of pipes where water flows can be visible or hidden.

The plants are further divided into two types: wet and dry. Wet and dry plants are further separated into two categories. One of the most prevalent is the wet plant. The pipes of this kind are filled with water that is dispensed under pressure in the event of a fire and continue to do so until a control valve is closed. The supply is dependent on a thermosensitive component that breaks when the ambient temperature reaches a range between 57C° and 77C°, resulting in water falling. The sprinkler activates the water supply in the event of a fire, and the alarm bell sounds to signal impending danger.

Water in pipes may freeze in extremely cold temperatures. A dry sprinkler system can be installed in these circumstances. With these systems, the pipes are pressured with air, and a valve stops water entry until the sprinkler is turned on in the event of a fire. In dry sprinkler systems, the pipes upstream of the control station are always pressurized with water, whereas the pipes downstream of the station are always pressurized with air. As one or more dispensers are opened, the air pressure drops, immediately allowing water to enter the distribution pipes.

Thus, dry plants have the same advantages as wet plants but are slower in spraying water when activated. In case of fire, the sprinkler system starts the water supply, while the alarm bell comes into action by setting off the alarm warning.



Sprinkler piping system

Smoke detectors

Smoke detectors come in two varieties: "ionizing chamber" and "optical beam" models. The variation in the electric field that is produced for the creation of ions in the air when there is a fire, allows ionizing chamber smoke detectors to detect the presence of smoke. These detectors work well in situations where fires spread quickly, such as when Molotov bottles are thrown. Also, we need to take into account the fact that churches are empty at night. Therefore, if they are lacking intrusion alarm systems or cameras, it would be very easy for an arsonist to break in and start a fire that, if not detected right away, could result in the complete destruction of the place of worship, seriously harming the local community's artistic and cultural heritage.

The optical beam smoke detectors work thanks to a particular phenomenon of optical diffusion of light, the so-called "Tyndall effect". The smoke that develops during a fire, invades the detector chamber and varies the way the light spreads inside, generating an alarm. They are not recommended for installation at the structures of interest because they are too subject to false alarms due to the low brightness of some areas.

Smoke detector

Fire extinguishers

Fire extinguishers are a crucial component in every building's safety system. Since that firemen need some time to arrive, they are the most secure technique of fire prevention and emergency response. Extinguishers come in a variety of types that vary depending on the sort of fire they must put out. It might be worth using both CO2 extinguishers placed at different parts of the structure and a large- capacity powder extinguisher, however this assessment must be done on a case-by-case basis with the assistance of a fire protection specialist consultant. It is advisable to differentiate in order to deal with many forms of fire that could arise during an assault or arson while still safeguarding the religious cultural heritage. It is obvious that using CO2 to put out a fire started by a Molotov cocktail bottle that spreads combustible liquid is different from trying to put out an arson fire that's been set on a main wooden door. Due to the vast scorched area in the second case and the possibility that CO2 may not be effective, dust is more efficient. Generally speaking, CO2 extinguishers can be used to put out small or liquid fires (like those started by Molotov cocktails), while powder can be used to put out larger fires, like those started by huge wooden structures. The many existing regulations require that the personnel in charge of using extinguishers attend a specialized training.

FIRE CLASS	TYPES OF FIRE EXTINGUISHERS		
	CO20	POWDER	FOAM
A - SOLID	✗ (large solids)	✓	✓
B - LIQUID	✓	✓	✓
C - GAS	✓	✓	✗
D - METAL	✗	✓	✗
E - ELECTRONIC DEVICES	✓	✓	✗
F - GENERAL OIL AND FATS	✗	✗	✗

CO2 extinguishers contain liquid compressed carbon dioxide. Air is drawn into the extinguisher when it is activated, and when the liquid is ejected, it turns into carbon dioxide snow. It is also known as "dry ice." The carbon snow changes once more and returns to gaseous form when it comes into contact with fire, subtracting oxygen and therefore suffocating it. When using these extinguishers, extra caution must be exercised in there are people around as they can lead to cold burns and breathing issues. At the same time, this factor should be kept in mind in the event of having to defend yourself against a potential terrorist, when fleeing is not an option.

On the other side, dust extinguishers are more ductile and effective at putting out practically all sorts of fire. They are highly effective at putting out fires caused by solid, liquid, gaseous, and metallic materials. They can also put out electrical appliance fires, however doing so results in permanent harm to the equipment. This kind of extinguisher also puts out fires by cooling and suffocating. When used inside a building, it can make people intoxicated and scatter a significant amount of extinguishing material in the area around 4 or 5 meters from the fire. As previously stated, when necessary, a transportable trolley fire extinguisher may be used. The CO2 extinguishers should be generally preferred because they produce less damages to the nearby materials than the powder.

Fire doors

In order to suffocate the fire and stop it from spreading, fire doors are built to withstand the heat of the flames and shut off the oxygen supply. Steel, plaster, glass, vermiculite layers, wood, and other combinations of these materials may be used to create these passive defences. The following are the purposes of fire doors:

- to stop the spread of fire and smoke within a building or between adjacent structures;
- to give building occupants a way out;
- to allow firefighters to intervene with some degree of safety;
- to facilitate the operation of active fire-fighting systems;
- to safeguard works of art and cultural landmarks that are situated in those areas.

Such doors must guarantee the following:

- Resistance: the door is flame-resistant and prevents the spread of fire outside the environment where it occurred;
- Hermeticity: the door prevents the

passage of the gases produced by the fire from spreading to other environments;

- Insulation: the door isolates the premises from the one where the fire developed, keeping the temperatures within set limits (about 150 C).

The doors can withstand fire for up to 180 minutes. Creating temporary safe spaces is a crucial additional application of fire doors. Moreover, some recent attacks on places of worship across various faiths have underscored that terrorists sometimes possess only knives, lacking access to firearms or explosives. In such scenarios, a sturdy fire door can effectively block access for an armed individual, offering safety until assistance arrives. This significance is heightened considering that panic rooms may not always be available within places of worship. Furthermore, doors can include extra functionalities like smart electronic locks activated solely by authorized individuals.

Intelligent electronic locks

An intelligent electronic lock is a home automation device that can be installed on all kinds of doors. Both internal and outdoor doors can have smart locks. These doors allow for access control and can be opened or not, depending on whether the individual attempting to gain entry possesses the required electronic authorization. These security systems can be managed remotely via a control panel or a mobile phone app. In the event of an attack, individuals in charge of the system can allow the police entrance by remotely opening the doors without putting themselves in danger. This also prevents the breaking through of historic doors or the use of explosives to break down walls by special forces attempting to access the place of worship.

Intelligent electronic lock is a user recognition device that can work in different modes. The most common mode involves connecting via Bluetooth or Wi-Fi to an app downloaded on the mobile phone. This app allows both remote control and automatic recognition of the phone in order to ensure access without having to perform any operation on the phone.

There are also locks with numerical access systems, voice recognition or fingerprint recognition. The most practical solution, in this case, seems to be that of cellular access.

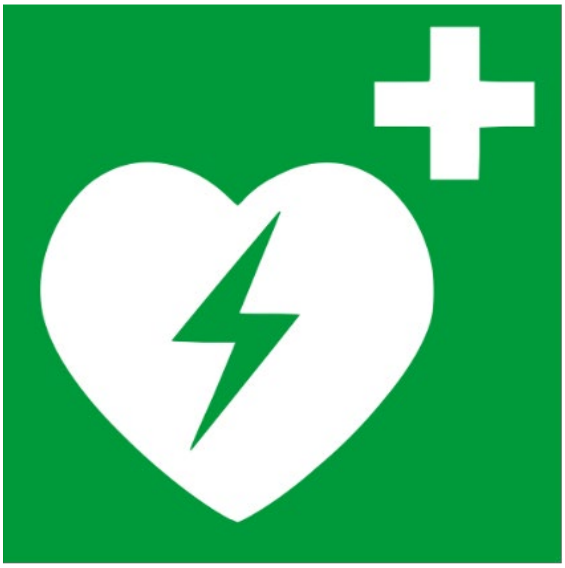
Intelligent electronic lock

AED devices

AEDs (Automated External Defibrillator) are a type of medical equipment used throughout Europe that are typically made available to users in areas where there is a mass exodus of people. It can be easily identified by its distinctive, high visible symbol and it can save life. AEDs are divided in two main categories:

- Automatic external defibrillator;
- External semi-automatic defibrillator.

There is only one "ON/OFF" button on the external automatic defibrillator. The AED will automatically assess the patient after applying the "PADS," or electrodes, and decide whether to deliver the discharge or shock or not. Via audio communications from the AED, the user and rescuer are kept constantly informed of the procedures carried out by the medical equipment and given guidance on any necessary steps. It is advisable to train some subjects on the use of such a device, as well as basic techniques of first aid (BLS-D). The person who decides to intervene during a terrorist attack should be aware that doing so can be extremely risky because some terrorists can be nearby. Therefore, it is strongly advised that individuals who choose to do so have at least a basic understanding of the risks of this kind of intervention.



AED device symbol

Panic buttons

A panic alarm is a simple-to-use electronic device that can be used to alert for assistance in an emergency if there is a risk to people or property. It is made to cut down on the amount of time before help can be provided. Often, but not always, a hidden panic alarm button is used to operate it. These buttons can be linked to a monitoring station, a local alarm system, or a bell or siren that can be heard. The alarm can be used to call for local security, police, or emergency services for aid in an emergency. Some devices can turn on, record or assess the event. These buttons are electrical devices with internal long-life batteries that are often waterproof, shockproof, and extremely durable. When pressed, many panic alarm buttons lock on and need a key to be reset. Others might experience a brief delay, during which the request for assistance might be cancelled.

The monitoring service operates a call centre that is open round-the-clock to take calls from the system console. Some monitoring systems use qualified operators who can more accurately assess the seriousness of support requests and choose whether to send an emergency service or handle the issue remotely.

An electronic device worn on a bracelet or necklace as part of a medical alert system is called a medical alert panic button or medical alarm. When activated, it wirelessly connects to a console in the house, dialling the alarm monitoring team to notify them of an emergency. The emergency services will be called in depending on the urgency of the issue, according to the alarm monitoring staff. The advantage of using an alert button in a medical emergency over a cell phone is that the person who is in difficulty might not be able to dial the emergency number or might not be able to speak.

In the event of a terrorist attack, this kind of emergency alert can be highly helpful because it enables victims, such as hostages held inside a place of worship, to transmit a silent alarm to the security forces. So, terrorists may face special forces when they least expect it. These should, of course, be utilized by those in charge of security and/or by volunteers who have special expertise in security.

Self-protection in the case of a terrorist attack

TOPIC	TIP
Keep a safe distance	It is crucial to prevent a suspicious individual from getting too close. This must be avoided especially by those who have a service gun, because the aggressor could attack them to take possession of the weapon. If a suspect approaches, it is important to prevent him from exceeding the minimum distance of one meter. If he does, it is necessary to back away. Those with service weapons should avoid putting themselves in positions where they could be taken by surprise.
Even if you are injured, run away	Even if you have been injured once, it is essential to run away immediately to avoid being hit further. Though it is unlikely that a single stab can kill a person, trying to escape remains vital in order to avoid any further injuries. Rather than trying to block the aggressor it is essential to get away from his radius of action, because if he is not at close range, his weapon serves no purpose and, having to chase the victim, will take away momentum to his attack.

In the event you are caught, wriggle	Feeling of fear, shock or surprise may take over those who are caught by a terrorist. In these cases, it is essential not to become overwhelmed psychologically and wriggle as much as possible to get away.
Shout or scream with all the breath you have in your throat	If you are attacked, start screaming to alert the surrounding people so that they can escape and call for help. This can also intimidate the attacker because it draws attention to him/her.
Use objects to protect and keep the aggressor at a distance	A bag can be used to parry stabs and a chair to keep the aggressor at a distance. Putting yourself behind a large object, such as a car or a table, can delay the aggressor's action and make it more difficult to reach the you.
If barehanded, protect youself from a knife attack using the outside of your forearms, kicking and keeping your fists closed	If you have to defend yourself with your bare hands from a knife attack, it is better to use the outside of your forearms and keep your fists closed, rather than your hands open. The forearms are more robust and less sensitive. If you fall, kick your feet as this can prevent the aggressor from jumping on you (the feet are protected by shoes).

A safe room, which could be locked from the inside, is a high valid alternative.

CONCLUSION

In summary, this is an overview of the main technical security measures that could be taken into consideration when protecting a PoW:

Mitigation measure	Location	Threat	Purpose
Sprinkler system	Internal	Fire	When the presence of a fire is detected, through a temperature detector once a heat threshold has been exceeded (usually between 68 and 74°C), the system is activated to extinguish the fire through a rain extinguishing and Sprinkler
Fire extinguishers	Internal	Fire	To allow manual intervention, possibly before the Sprinkler system is activated
Interna fireproof partitions	Internal	Fire	Prevent interior partitions, countertops from fireproof

Furniture materials	Internal	Fire	Prevent carpets, curtains, fabrics, cushions from being fireproof
Fire Alarm / Smoke detector	Internal	Fire	Promptly report the fire when there is anyone in the House of Worship
Fire doors	Internal	Fire / Assault	They prevent the spread of fire and provide robust protection behind which to shelter in case of assault
Windows	Internal	Attack	All accesses to the outside, if present or glazed, must be shatterproof and opaque so as to obstruct the view from the outside as well as for windows
Emergency exits	Internal / External	Any emergency	Prepare escape and alternative routes according to local regulations with anti-panic safety doors or in the presence of separating compartments with REI doors with a minimum seal of 60 minutes.
CCTV	External	Attack	CCTV closed circuit camera system connected via WiFI with separate power supply from the mains and the base not located on the ground floor. The basic requirements give the possibility of monitoring 24/24 even remotely, alarm sensors, infrared equipment for the night and the possibility of recording in the cloud.

Backup Generator	External	Any emergency	Keep the systems running even if the main power supply is cut off.
Anti-ramming barriers / gates	External	Vehicle attack	Mobile shatterproof barriers to prevent possible vehicle attacks. In the majority of cases, where this is not possible, it would be enough to close the access gate to the site with gates.
Lighting	External	Any emergency	Supplementary lighting powered by an alternative source to the primary one is a deterrent to many vandalism attacks
Training	Human resources	Any emergency	Supplementary lighting powered by an alternative source to the primary one is a deterrent to many vandalism attacks
Safety emergency procedures	Human resources	Any emergency	They are essential to make the community of the faithful and religious leaders aware of what to do in case of emergency and above to prepare them to carry out the previously developed procedures.
Security App	Human resources	Any emergency	A system to connect the believers with an App to communicate emergencies in connection with the Police

The religious communities cannot be easily categorized since they are neither governmental or private sector organisations. They have usually huge and outdated infrastructure and lack professional knowledge in the field of safety and security. This is clearly understandable as their interest lies in religion and not in safety and security.

What it has been stressed here is that **unfortunately religious communities have been, are and will be a target of violent and terrorist attacks and religious leaders, as well as the other local stakeholders, need to be aware of these threats to ensure that such communities can preserve their freedom and enjoy their religious and community life safely.**

06

IN THE AFTERMATH OF AN ATTACK

Protocols on crisis management

Despite all the prevention and safety measures presented in this handbook, **violent or terrorist acts may still occur**. For this reason, we thought it valuable to add a last chapter on the important role played by religious communities' leaders, local policymakers and LEAs representatives in the aftermath of an attack. These attacks, as any other traumatic events and irrespective of their source or scale, have the potential to **cause distress and they have the greatest impact on the affected local community**.

In the most severe cases, all the national authorities have **protocols or plans for crisis intervention** to activate immediately, with the aim to manage and coordinate the first responders, integrating national, regional and local governance structures.

Regardless of the severity of the attack suffered, **the consequences can be mitigated by effective political, religious and civil leadership with an intervention capacity aimed to strengthen community cohesion and social support to victims and survivors**. In fact, there is evidence in scientific literature indicating that the way in which people's psychosocial responses to disasters are managed may be a defining factor in the ability of communities to recover. So, activities - in the short, medium and long term - that normalise reactions, protect social and community resources and signpost access to additional services are fundamental to effective psychosocial responses.

See this non-binding guidance by NATO Joint Medical Committee, on Psychosocial Care for People Affected by Disasters and Major Incidents: a Model for Designing, Delivering and Managing Psychosocial Services for People Involved in Major Incidents, Conflict, Disasters and Terrorism.

https://www.coe.int/t/dg4/majorhazards/ressources/virtuallibrary/materials/Others/NATO_Guidance_Psychosocial_Care_for_People_Affected_by_Disasters_and_Major_Incidents.pdf

Supporting the victims and community resilience

Once emergency care has been provided to victims, survivors and family members of a person whose death was directly caused by a violent or terrorist offence, their **specific needs** must be assessed:

- Recognition and respect of their role as victims.
- Support: medical care, specialised psychological-trauma care, information, practical assistance, legal assistance, communication (media) support, peer support, etc.
- Protection: physical protection, protection from secondary victimisation.
- Access to justice: safe participation in the criminal justice process.
- Compensation and restoration: financial compensation and help with the financial impact of a violent or terrorist attack. Restoration includes overall recovery and restorative justice processes.

Individual victims' needs will depend on personal characteristics; age; (mental) health; social network; socio-economic situation; cross border situation; and daily stressors. These needs will evolve over time, therefore, responding to the needs of victims of terrorism requires an **individualised victim-centred approach**.

On 18 January 2021, the Commission published the EU Handbook on Victims of Terrorism produced by the EU Centre of Expertise for Victims of Terrorism. The EU Handbook aims to assist national authorities and victim support organisations in the practical implementation of the EU legislation, based on lessons learned from responses to previous terrorist attacks. It is available here:

https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-centre-expertise-victims-terrorism_en

Furthermore, The National handbooks complement the EU Handbook on Victims of Terrorism (published in January 2021) and elaborate on the rights of victims of terrorism in each Member State. In particular, they include advanced or system-specific examples, with information and practical tools, in the domestic context of the Member States. They are available here:

https://commission.europa.eu/publications/eucvt-national-handbook-victims-terrorism_en

If violent or terrorist attacks always undermine social and cultural cohesion, this is even more true and profound when the target is a place of worship. We therefore recommend a **broader action of social accompaniment and social rehabilitation** aimed not only at the victims, but also at the local community as a whole.

These kinds of attacks, in fact, may often promote polarisation which divide communities and which can lead some to become radicalized. So, **an effective political, religious and civil leadership should take care of their communities' resilience**, as highlighted in the early prevention's practices and programs within chapter 3.

Furthermore, maintaining a strong and continuous interreligious dialogue, with periodic meetings between local religious communities, is ever more important to mitigate polarisation and radicalisation not only when a terrorist attack occurs locally impacting one of the communities, but also when the attack occurs far away causing a vast international echo, as in the case of the past and present wars in the Middle East.

07 SHIELD PARNERS

SYNYO GmbH

Web site: *synyo.com*

Zanasi & Partners

Web site: *zanasi-alessandro.eu*

Fundacja Obserwatorium Spoleczne

Web site: *obserwatoriumspoleczne.pl*

FUNDEA

Web site: *fundea.org*

Institutul Intercultural Timisoara

Web site: *intercultural.ro*

TECOMS

Web site: *tecoms.it*

Spin System

Web site: *spinsystem.eu*

HochschuleFürDenÖffentlichen Dienst in Bayern

Web site: *fhvr.bayern.de*

Município do Barreiro

Web site: *cm-barreiro.pt*

Europe Islamic Association

Web site: *euroislam.eu*

Institute for the Study of Global Antisemitism and Policy - Europe

European Organisation for Security

Web site: *eos-eu.com*

Polskie Towarzystwo Oceny Technologii

Web site: *ptot.pl*

Itapol Vigilanza

Web site: *italpolvigilanza.it*

Centro Internazionale di Ricerca Sistemica

Web site: *ricercasistemica.org*

Fondazione Amici della Cattedrale di Novara

Web site: *novaria.org*

Glavna Direktsia Natsionalna Politsia

Web site: *gdnp.mvr.bg*

Orszagos Rabbikepzo Zsido Egyetem

Web site: *or-zse.hu*