POLIZEI
BERLIN

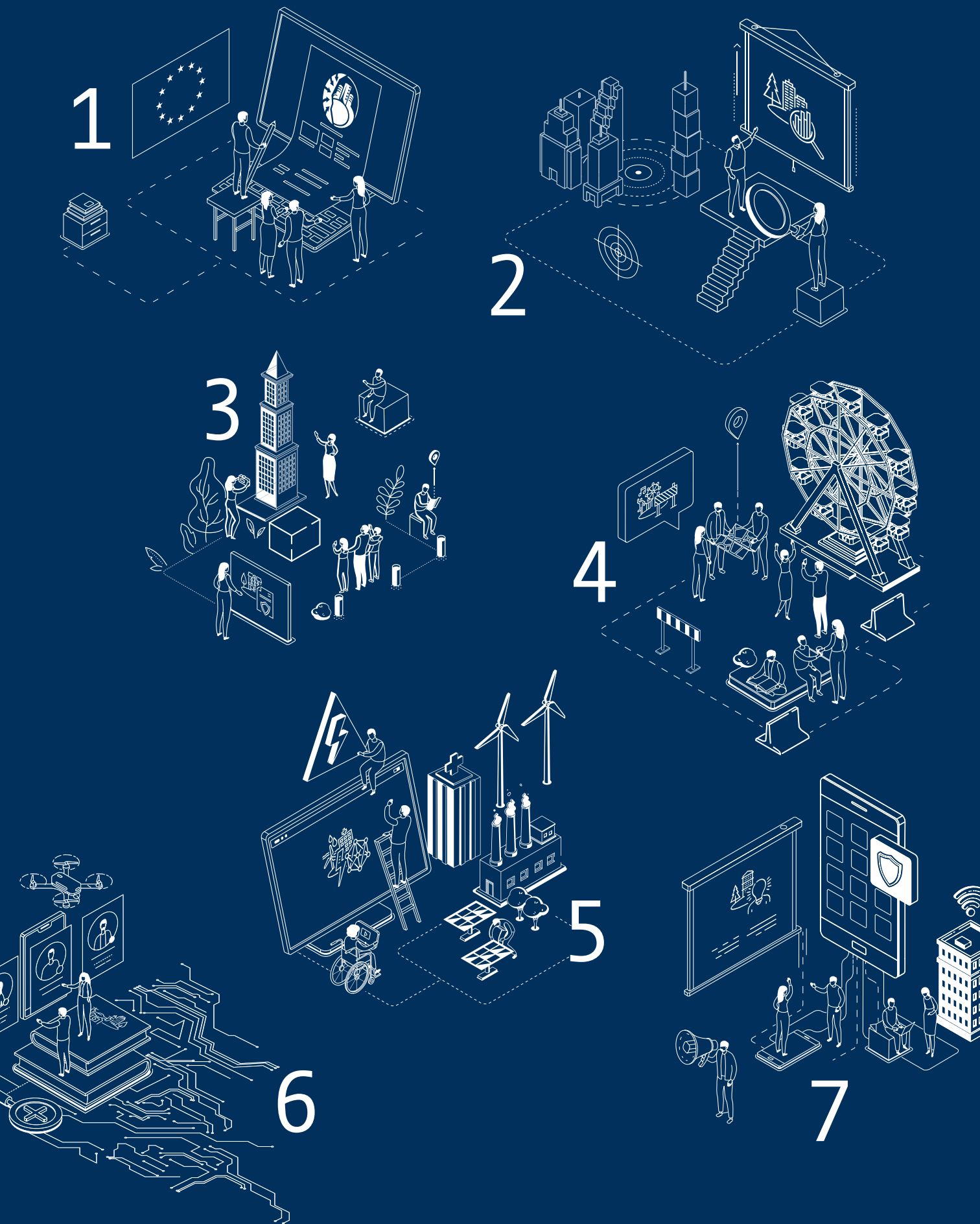*SafeCi*
Safer Space
for Safer Cities

European Recommendations for the Protection of Public Spaces against Terrorist Attacks

Content

Preface

,,

The world is becoming increasingly turbulent. Safety and security in general seem to be at stake more than ever before. SafeCi has brought together police authorities, scientists, and players from a variety of disciplines. The results of this co-operation are a manual, a vital network, and close contacts that have been formed in the process. At the same time, these results epitomize a successful and very efficient European co-operation. Thank you very much to our partners.

Dr. Barbara Slowik, Police President Berlin Police

Germany

Since the mid-2000s, all of Europe has been experiencing recurring moments of shock that has brought home to the world at large the vulnerability of the liberal-democratic state systems in Western societies. The attacks on our metropolises have caused deep concern and manifold responses in the security architecture of European nations. Europe's public spaces are now the target of various forms of terrorist attacks – these public spaces are unprotected and freely accessible to everyone. The European police and security authorities are faced with the same challenge: to effectively protect our citizens against violence and attacks without restricting their quality of life and dampening their spirit too much. When the idea for the project "Safer Space for Safer Cities" (SafeCi) gradually took on shape, we were determined to defend our democratic values and to do our part to safeguard the security in our cities against the backdrop of current threats.

United by this objective, we succeeded in putting together a multinational and interdisciplinary project team comprising experienced police officers, experts, and scientists. Together, we were able to look at, discuss, and analyse promising potential solutions in the partner states: technical know-how, police experience, scientific concepts, commercial ranges of goods on offer, and diverse approaches contributed to our joint work or were taken into consideration.

In an increasingly complex world, we must bundle our competence, join forces, and think transnationally. SafeCi has structured the existing know-how and provides a comprehensive European overview. Thus, we make an effective contribution to the protection of public spaces. We do not limit ourselves to pointing out a one-dimensional solution. Rather, this manual is about reflecting the multitude of options and perspectives – knowing full well that in light of the dynamic technical developments it is not possible to consider every aspect in its entirety.

In March of this year, the world at large and the microcosm of our project were hit by the Corona pandemic: since then, we have been part of an exceptional situation never experienced before, which brings home in particular to all of us how important public spaces are for our coexistence and for democracy. All of a sudden, public spaces were deserted and things we took for granted in terms of our social life were taken from us. Travelling was no longer possible, exchanging ideas in an international team became a lot more difficult – but we never lost sight of our objective.

The result of all parties involved is now before you: European recommended courses of action for the protection of public spaces against terrorist attacks. We are optimistic that these can provide important stimuli for successful security work to protect public spaces in Europe and would be delighted if European police and security authorities used our collection of practical examples for their work.

Ultimately, legal, political, social, and cultural conditions will determine which protective measures can be implemented in the individual states. This protective effect begins in the minds of a society and its leaders. The basic requirement is the mindset: security must be wanted, but in many respects – be it monetary, aesthetically or emotionally – it comes at a price. If we want security, much can be done. It is up to each society individually to negotiate and find the balance.

We would like to thank all contributors and partners for their exceptional dedication and their flexibility. Our joint European journey has not come to an end – we are now interconnected more strongly than before and will explore new avenues together.

Stefan Majchrzak and Mario Hornig
SafeCi Project Leaders

The project consortium comprises ten international partners that are briefly introduced in the overview below.

	Responsibility	Personnel	Annual budget
An Garda Síochána	national	18031	€ 1.5 bn
Ireland			

	Responsibility	Personnel	Annual budget
Police Lëtzebuerg	national	2400	€ 240 m
Luxembourg			

Police Bruxelles-Capitale-Ixelles	local	2636	€ 240 m
Belgium			

Polícia de Segurança Pública	national	22377	€ 800 m
Portugal			

Policie České republiky	national	49700	approx. € 1.7 bn
Czech Republic			

Polismyndigheten Police Region Stockholm	local	7200	€ 508 m
Sweden			

Helsingin poliisilaitos	local	1690	€ 123 m
Finland			

Guardia Civil	national	80000	€ 3 bn
Spain			

State Police Division Vienna	local	6400	€ 600 m
Austria			

Berlin Police	local	26000	€ 1.5 bn
Germany			

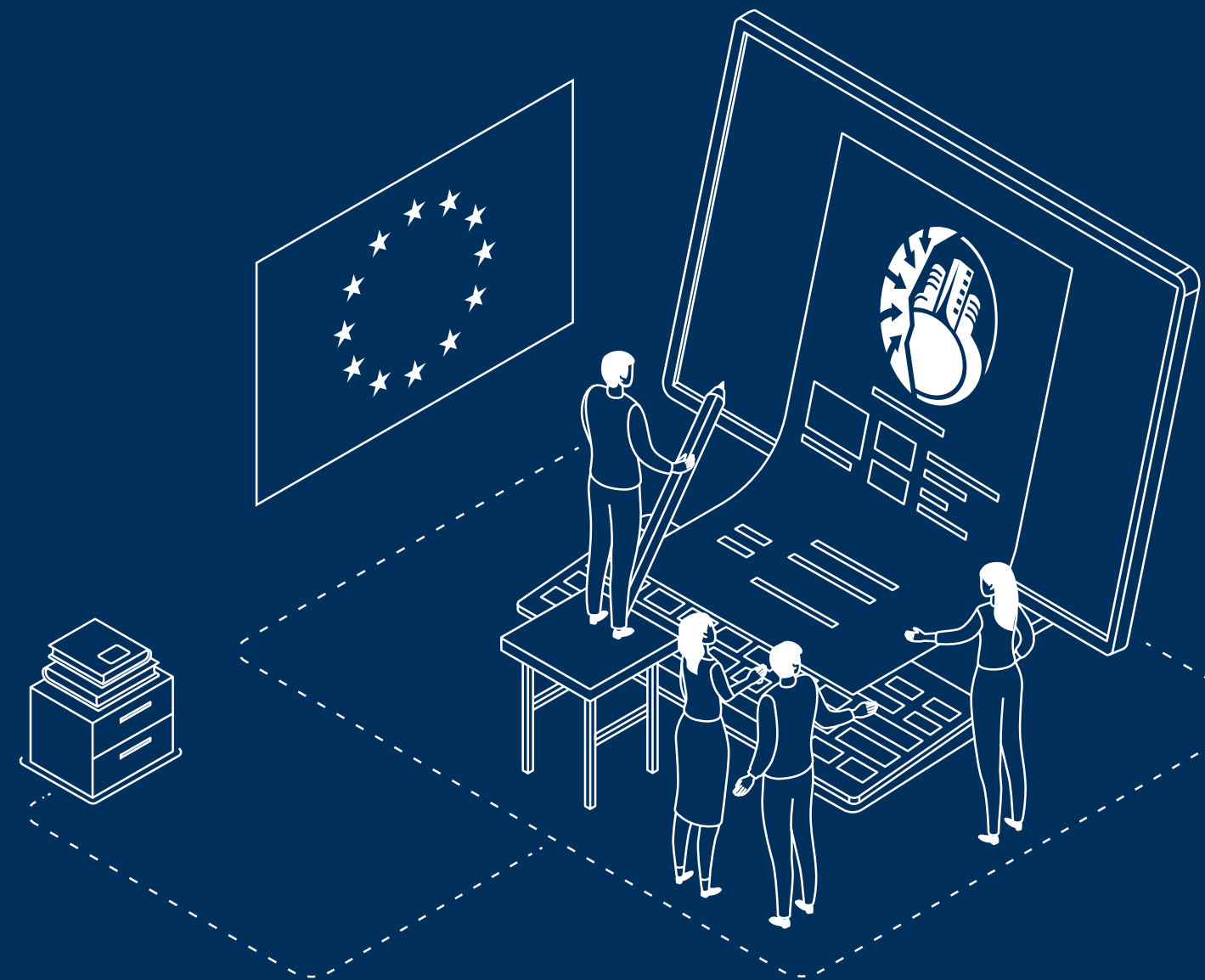# Safer Space for Safer Cities – A European Security Project

"

Our only chance against the current threats is to face them together at the sharp end right from the very beginning. Exchanging knowledge, good practices, and experiences in the context of real co-operation is the key to success. In the end, a hand is always stronger than five fingers.

Lieutenant Colonel Jesús Gayoso, Head of the Rapid Action Group of the Guardia Civil (26 April 1971 – 27 March 2020)

Lieutenant Colonel Jesús Gayoso died as a result of a Corona infection. He always supported the international co-operation of police authorities in their fight against crime and terrorism and thus actively advanced it. His death is a tremendous loss to the entire European police force.

Spain

Background

Safer Space for Safer Cities (SafeCi) is a European prevention project. It describes, from the perspective of police and security authorities, how public spaces can be better protected against terrorist attacks and comparable threats.

EU Action Plan (18/10/2017)

The EU Action Plan intends to support the protection of public spaces as part of the European Union's security strategy. In October 2017, the European Commission published a call for project proposals for improving the protection of public spaces. For this purpose, a total of EUR 18.5 million was provided from the Internal Security Fund.

Definition: Public Spaces

Public spaces are all places publicly owned or of public use, accessible and enjoyable by all for free and without profit motive. This includes streets, open spaces and public facilities.

(UN-Habitat Global Network on Safer Cities)

The phenomenon of threats to public spaces by terrorist attacks within Europe is not new, but has escalated significantly in the last decade. This is largely down to the increase of acts of violence with a jihadist motive, which came to a head in the years 2014 to 2017. In recent years, international – and in particular Islamist – terrorism has become one of the greatest challenges for Europe's security policy.

The primary attack targets are "soft targets" such as crowds. Public spaces are particularly affected for three main reasons: they are usually easily accessible, they tend to be frequented by many potential victims, and they often have a symbolic character. In addition to the actual consequences of the attack, attacks on public places have a significant negative impact on the sense of security among the general public. This is part of the attackers' strategy.

When looking at the design of public spaces, a global paradigm shift is becoming obvious – with the aim of increasing the attractiveness of public spaces as the main quality criterion of urban life while at the same time increasing their security.

The question of how to ensure security without restricting people's quality of life must be answered by the competent security authorities, the political decision makers, and ultimately by society as a whole. However, this question addresses a dilemma that cannot be solved easily as security and freedom are conflicting priorities.

Safer Space for Safer Cities | EU

A European Security Project

Upon the initiative of the Senate Department for the Interior and Sport in Berlin, the Berlin Police devised the European Best-Practice project "SafeCi – Safer Space for Safer Cities". The overall control rests with the Berlin Police.

Aimed at: executives, practitioners from security authorities, political decision makers

Objective:
- Knowledge transfer between the SafeCi partners and other cities and states within Europe about measures for the protection of public spaces
- Development of innovative measures for the protection of public spaces
- Establishing long-term networking activities between the European partners

Method:
- **Questionnaires covering different core topics (cf. Chapters II to VII)** were developed. The six superordinate levels of content were: law, technology and practice, tactics, finances, society and psychology, co-operation and communication.

- **13 study visits** to a variety of public spaces in Europe and Israel were a core element of the project. Mixed teams from the partner countries assessed and examined these places by means of a methodical guideline developed by SafeCi.

- **In several workshops** the content prepared was discussed with the project participants and invited experts. The consortium recorded the results in the form of a manual.

An Overview of the SafeCi Project Results

→ **The protection of public spaces is a highly complex topic.** There is no one universal solution that can be applied to all locations as the underlying local conditions and utilisation scenarios vary too much.

→ **A structured approach is essential.** This includes a risk and threat assessment beforehand. As part of the concept, it is also wise to combine several measures.

→ **When designing public spaces, security aspects have to be taken into consideration from the outset.** Security authorities can be involved in an advisory capacity early on.

→ **Experiences from current terrorist attacks should be incorporated into existing concepts.** Ultimately, each completed terrorist attack affects the entire European society living in freedom.

→ **Innovative approaches should be checked and applied.** Technical progress always affords new possibilities to increase the protection of public spaces.

→ **The protection of public spaces must be understood as a dynamic and ever-changing issue.** Security authorities should continuously adjust to these changes.

→ **The implementation of security measures should be flanked by a process of weighing up the conflicting interest of freedom and security.** The resilience of public spaces must be improved without affecting their character as freely accessible spaces to be enjoyed by everyone.

→ **The use of public spaces can be increased by integrating the general public and raising awareness.** The acceptance of police measures can also be increased.

→ **The international exchange between partners makes it easier to keep up to date with current developments.** Across Europe, there is a multitude of good and innovative police concepts for the protection of public spaces.

→ **The only way to counter modern terrorism as a transnational threat is by expanding international co-operation in Europe.** Thus, projects such as Safer Space for Safer Cities make a valuable contribution to the security of Europe.

> The issue of SafeCi affects all of Europe. The project provides us with the opportunity to get together and develop long-term prevention measures for the protection of public spaces – and integrate structural measures and the latest technologies as well as risk analyses, measures for event security and innovative alternative measures in the process. To enable us to create a safe and secure environment for everyone, we should discuss the existing challenges together.

Ann Marie Cagney, Assistant Commissioner An Garda Síochána

Ireland

2 Risk and Threat Assessment for Public Spaces
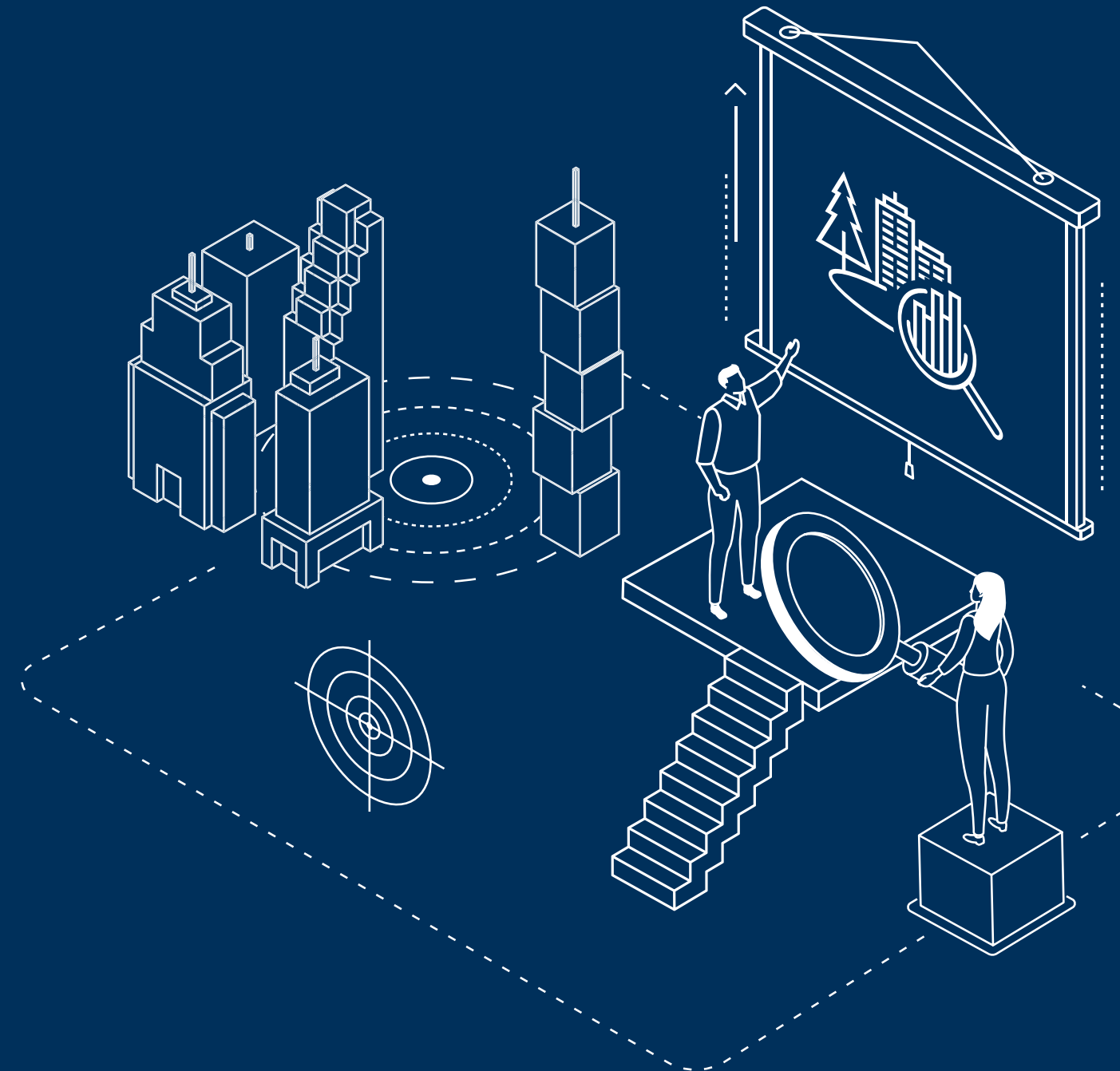
Introduction

The probability of a person in the EU becoming the victim of a terrorist attack is negligible.

During the last decade, a total of **119 Islamist terrorist attacks** were completed, failed or foiled in the European Union. In the course of these attacks, **382 people were killed.**

That means that during the last decade an average of **38.2 people** per annum were victims of religiously motivated/jihadist terrorism in the European Union. Given the current number of approx. **513 million EU residents,** this means approx. **0.07 people** per one million.
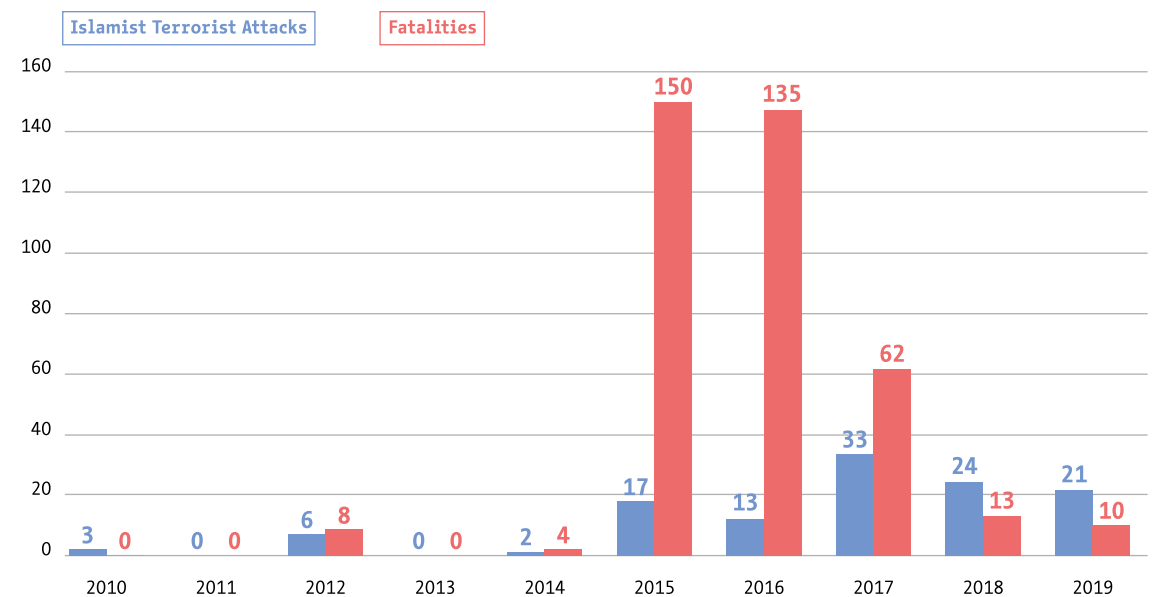
Why then does the discussion of protecting public spaces from terrorist attacks take up so much room?

Does it even make sense to think about protective measures to this extent, even though the likelihood is still remote?

The answer is: Yes

+ People have a strong need for security: According to a public opinion poll of the European Commission, 95 percent of the interviewees considered anti-terrorism measures one of the most important tasks with regard to internal security in the EU.

+ Terrorism is not just an attack on our lives or our physical integrity but also on our society as a whole and our European value system.

Islamist Terrorist Attacks / Fatalities

Year	Islamist Terrorist Attacks	Fatalities
2010	3	0
2011	0	0
2012	6	8
2013	0	0
2014	2	4
2015	17	150
2016	13	135
2017	33	62
2018	24	13
2019	21	10

Challenges

How can we make well-informed decisions about the avoidance, mitigation, postponement or acceptance of risks? The basis for such decisions is the systematic process of risk management, which is intended to ensure the structured, continuous, and efficient handling of existing threats. Security risks such as the risk of terrorist attacks can be checked and controlled in the context of a comprehensive process divided into different stages and individual steps. This process provides a (pre-structured) tool to identify, analyse and evaluate security risks and offers support for developing and implementing cost-efficient security measures with the general goal of mitigating the identified risks.

In the European Union, security risk management can be performed at European, national and local level. The following description of the risk management process focusses on the local or urban level as the protection of public spaces has priority, which is generally the responsibility of local security authorities.

Risk Assessment comprises those steps of analytical preparatory work that are needed for decision makers in politics and security authorities taking action. It comprises three steps: identification, analysis, and assessment of security risks.

Step 1

Risk Identification

For which threat is the risk to be determined, which threat protection is needed? To identify such scenarios, the first step is to analyse completed, foiled, and failed terrorist attacks.

As a framework of reference, content-related, spatial, and temporal parameters are applied.

A synopsis of the Islamist terrorist attacks completed or failed in the EU since 2004 reveals the following methods of committing attacks:

+ Bomb and arson attacks, firearms attacks, attacks with cutting and stabbing weapons, attacks with cars/trucks.
+ Attacks with biological or chemical weapons (taking into account planned attacks that were uncovered and foiled).
+ Attacks with drones (taking into account potential future "trends"; insights such as terrorist attacks outside the EU might offer clues).

Step 2

Risk Analysis

Risk analysis is the core element of risk assessment and a central cornerstone of the protection of public spaces. It allows for a systematic determination of probability and the corresponding likely impact. On this basis, different risks can be assessed and systematic, effective protective measures taken.

Elements of risk analysis:

+ Determination of safety goal: Which spatial area and which subjects of protection are to be protected to what extent?
+ National threat assessment: How are the threats for the entire country assessed regarding particular risks? This forms the basis for recommended courses of action to be developed for the government and also security authorities at regional and local level.
+ Local threat assessment: Which specific threat environments (e.g. city, main shopping street, certain event) is the focus on?
+ Vulnerability analysis: What are the weaknesses, "vulnerabilities", of a potential attack target, which make this more vulnerable to the destructive consequences of attacks and there by affect the risk level directly?
+ Determination of probability: How likely is an attack – based on the results of the local threat assessment and the vulnerability analysis?
+ Determination of impact: What impact is to be expected when individual threat scenarios occur? Which subjects of protection will be damaged and to what extent?

Step 3

Risk Assessment

The objective of risk assessment is to provide decision makers in politics and security authorities with reliable information on threats and associated risks in the form of a neutral and transparent decision-making basis, thus enabling them to make adequate decisions about how to respond to these risks.

Following the risk analysis – after determining the probability and the impact for the individual threat scenarios -, the risk can then be assessed with the help of the matrix below.

Risk Response

The stage of risk assessment is followed by the stage of risk response – with the following steps:

+ Basic decision about how to respond to the individual risks. (Avoidance, mitigation, postponement or acceptance?)
+ Development and implementation of protective measures.
+ Continuous control of the quality and effectiveness of implemented measures.

+ Checks as to whether any remaining residual risk seems acceptable in light of the defined safety goals.
+ Review and update of the entire risk management process with clearly defined responsibilities.

The decisions to be made in the context of risk response should be made on the basis of a solid cost-benefit analysis.

In order to include political and social interests, deliberations should be communicated between the security authorities, politicians, the general public and scientists. Social acceptance can then be achieved by means of dialogue during the decision-making process.

EU Vulnerability Assessment Tool (VAT)

In order to support the EU Member States in the protection of public spaces and the vulnerability analyses required for this purpose, the Directorate-General Home of the European Union developed the EU Vulnerability Assessment Tool (VAT). Basically, this works like a checklist: It allows for a comprehensive and clear assessment of a public space in terms of its vulnerabilities and points out possible protective measures. The VAT is currently tested and assessed in five European cities.

Risk Assessment

Probability	Extent of damage				
	Low	Moderate	Substantial	Severe	Critical
Critical	Substantial	Severe	Severe	Critical	Critical
Severe	Substantial	Substantial	Severe	Severe	Critical
Substantial	Moderate	Substantial	Substantial	Severe	Severe
Moderate	Moderate	Moderate	Substantial	Substantial	Severe
Low	Low	Moderate	Moderate	Substantial	Substantial

Risk Matrix

Impact — Critical 5, Severe 4, Substantial 3, Moderate 2, Low 1

Probability — Low 1, Moderate 2, Substantial 3, Severe 4, Critical 5

Good Practice | Belgium

Coordination Unit for Threat Analysis (CUTA)

CUTA is an independent national institution that is responsible for the general, strategic and case-specific assessment of terrorist and extremist threats in Belgium.

Aimed at: Police authorities of the country and numerous other authorities that share responsibility for state security

Objective: Based on CUTA assessments, the affected institutions can take the necessary measures to fend off threats. CUTA itself does not take action.

Method: Based on information and intelligence communicated by the partner authorities. Information is exchanged with foreign partner authorities and relevant intelligence forwarded to the Belgian authorities.

Three kinds of assessments are performed:
- general – published monthly
- strategic – for critical infrastructures
- case-specific – for individuals, groups, institutions and events

If a threat assessment is requested by a partner authority, CUTA initially gathers all relevant information and intelligence. The information is then analysed and evaluated by means of a risk matrix. The result of the assessment is shown as a threat level (Level 1 to 4) including further explanations of the assessment process.

Good Practice | EU

EU Protective Security Advisors Training

The EU Protective Security Advisors Training is a programme developed by the Directorate-General Home of the European Commission.

Aimed at: EU Security Advisors whose role is to perform vulnerability assessments across Europe.

Objective: Networking and exchange of information between the security authorities, international partnerships and co-operation, strengthening the security of public spaces. Assessments of the external advisors and the experience-based knowledge of the local players are translated into a holistic security concept.

Method: EU member states have the opportunity, by invitation, to have a vulnerability assessment performed on-site by an international and interdisciplinary panel. The panel identifies vulnerabilities, recommends courses of action and points out potential protective measures. Whether the recommended measures are implemented is up to the member state.

Recommendations

+ **Will firearms or drones be used?**
+ **Which locations will they attack?**
+ **Which effects would a hostile vehicle ramming have compared to a knife attack?**

The complex field of risk assessment tries to approach these kinds of basic questions by using a variety of methods. Risks are determined and weighted. Usually, there are not enough resources to reduce or neutralise a risk.

The difficulty consists in developing a security strategy that balances out both security and freedom. The instrument of risk management can play an important role in this context.

→ An analytical approach initially allows for an identification and reduction of the greatest risks instead of trying in vain to protect everything.

→ In general, existing knowledge must be expanded, the development of supporting analytical tools must be expedited and the individual steps of risk management must be institutionalised further.

→ Empirical data offers not just valuable insights but is also a fundamental basis for the analytical work of the security authorities.

→ The protection of public spaces must take into account the conflicting priorities of security and freedom.

"

In our ever-changing world, terrorism threatens everyday life in a Europe that has opened its borders to welcome guests. This, in turn, presents increased challenges for police work in the field of public security. SafeCi offers the participating partners the opportunity to learn and develop: by responding to threats from the recent past and preventing them.

Manuel Augusto Magina da Silva,
National Director of the Polícia de Segurança Pública

Portugal

3 Structural Protection of Public Spaces against Terrorist Attacks

Introduction

There are many options; the crucial factor is a continuous, interdepartmental and interdisciplinary co-operation.

Around two thirds of the world's population live in urban spaces – a trend that is going to increase in the decades to come and will also bring about change in the use of public spaces. This development demands long-term concepts for the future design and protection of urban spaces.

The focus of the terrorists' target selection has shifted to unprotected, primarily civilian attack targets, "soft targets". Therefore, there will be a stronger focus on the protection of public spaces again, especially against terrorism, and in particular on hostile vehicle rammings.

But how can public spaces that cannot be clearly contained be secured against an abstract threat? Tried and tested concepts for vehicle access control and perimeter protection can only be applied to a limited extent, as protective measures for all public spaces are not feasible financially or in terms of urban development and would probably meet with little acceptance among politicians and the general public. In general, it is not possible to predict trends and make prognoses, even if attacks always offer potential for copycat attacks. Attacks per se cannot be prevented by passive security measures. At best, they can be made more difficult in their implementation, mitigated in their impact or displaced to another location.

Challenges

The greatest challenge for the structural protection of public spaces is to agree on the best compromise that combines security with freedom, aesthetics and functionality – a compromise that can thus be backed by everyone involved. Multifunctional and integrative security solutions that blend in with the cityscape should combine as many interests as possible.

The three major objectives:

✚ Reduce the attractiveness of public spaces as potential attack targets

✚ Increase resilience against all possible forms of terrorist attacks

✚ Strengthen resilience in case of an attack

The different aspects of the structural protection of public spaces, presented below, provide an overview of this complex issue.

Structural Protection against Terrorist Attacks

The critical question is not what has to be done for the protection of public spaces but what can be done – and how to arrive at a balanced decision. The decision-making process should include financial resources, social and political acceptance, structural conditions, and restrictions arising from the use of that space.

What makes it so difficult to secure public spaces, even in the case of a generous budget and many options, is the number of variables that must be taken into consideration for any plans. For that purpose, it is worth taking a look at selected core disciplines of structural security.

Perimeter protection

The basic principles of perimeter protection also apply to the protection of public spaces against terrorism: deter, detect, delay, mitigate, respond. Ideally, for example, the deterrence of potential attackers is not be achieved by means of impressive security measures but rather by means of an unattractive attack target. Identified vulnerabilities can then be mitigated systematically by applying individual measures or a combination of different options, e.g. by systematically diverting crowds, changing vehicle access, design measures or special surveillance. For the protection of public spaces, special attention should be paid to deterrence.

Vehicle access control

The structural protection of public spaces against hostile vehicle rammings is often mentioned in the same breath as vehile access control, although a distinction should be made here. With regard to vehicle access control, measures of systematic traffic routing are complemented by various structural measures. These ensure a predefined measure of security, especially when tested and certified models are used.

Road safety

The insights from the discipline of road safety can provide a cheap alternative to structural vehicle access control – in particular, when considering that the energy of a vehicle quadruples when its speed doubles. People are used to the sight and benefits of traffic measures and these measures can cover several risk areas, such as the protection of pedestrians and cyclists at the same time. With regard to issues such as traffic turnaround, alternative means of transport, and autonomous driving there will be significant changes in the future. This includes, inter alia, the establishment of larger pedestrian zones or purely residential traffic.

This development could even call for considerations about the systematic installation of traffic bollards throughout city centres into question.

Urban design and crime prevention through environmental design

Securing public spaces against terrorist attacks is one aspect of crime prevention through environmental design (CPTED) that has recently been taken more and more into consideration. However, it is not the primary and sole objective of CPTED. The objective of protecting buildings against terrorism may even conflict with other objectives of CPTED. Implementing measures to increase visibility and accessibility for example may also increase the vulnerability to terrorist attacks as vehicles, blast waves, flying debris and projectiles encounter fewer obstacles and there are fewer options to take cover or escape. Also, clearly visible security measures such as bollards and fences may also have a negative effect on the sense of security as they may create the impression of being in a particularly vulnerable space.

However, structural measures to protect public spaces and other aspects of CPTED can also be planned by mutual agreement and implemented in such a way that public spaces become more enlivened and safer at the same time.

Possibilities for the Structural Protection of Public Spaces

The market offers a vast number of innovative possibilities for a structurally safe design of public spaces, too. A predefined safety goal can often be reached through a combination of different measures. The following points provide an initial overview of some structural possibilities for averting abstract threats.

Technical vehicle security barriers

The selection of available vehicle security barriers is great and the differences are significant. Bollards are among the oldest and most common methods for influencing the approach to an area to be protected. They can be static or mobile. Depending on the region, the distance between two bollards is stated as at least 120 centimetres, the height is 90 to 110 centime-

tres. In terms of the required installation depths, the products vary greatly: while shallow-mount bollards require installation depths of around 20 centimetres only, retractable bollards need up to 200 centimetres.

Reinforced street furniture

Street furniture is an innovative approach that can combine protection and aesthetics. In addition to its actual function (e.g. seating, bicycle stand, flower pot, raised flower bed, bus stop, kiosk, street light or billboard), it also often serves as a design feature – or even street art.

Street furniture is also used systematically for CPTED, for example to define occupied zones, enliven spaces, prevent dilapidation due to use or to prevent places causing anxiety. And their dual function as vehicle access control has been in use for some time now – albeit more to deter unauthorised vehicles and parking offenders than terrorists.

To ensure efficient hostile vehicle mitigation, structural reinforcement and firm anchors in the ground are required. Otherwise, benches for example would increase the danger in case of a vehicle impact, rather than reducing it, by becoming missiles themselves.

In case of an abstract threat, a selective approach is possible. Reinforced and certified products could be used at potential attack targets while sticking with cheaper and more delicate solutions in other areas.

Measures to protect public spaces against abstract attack scenarios do not follow predefined rules. They may, for example, also provide effective security in the depth of a room by providing cover for people, presenting an obstacle to vehicles or influencing behaviour directly. The clear advantages of street furniture compared with other constructional solutions are their multi-functional characteristics. Innovative concepts may even develop into tourist attractions. Stockholm, for example, uses larger and more massive models of the city's coat of arms ("Stockholm Lions") as vehicle security barriers in pedestrian zones. There is also innovative street furniture for protection against explosions and firearms.

Crowd management measures, warning and alarms
The fact that people often choose the shortest route and prefer certain options for sojourning can be taken advantage of: By means of systematic observation, tests and software simulation, preferred routes and occupied zones can be ascertained and subsequently be influenced. Thus, areas with increased pedestrian density can be promoted or prevented, routes specified and critical bottlenecks alleviated. Some countries are currently testing technical developments that can detect dangerous situations such as panic, flight, explosions or shots by means of pictures and noises and distinguish them from everyday situations.

The Planning Process

In order to develop an application routine for the planning process, which is suitable for everyday use, some aspects have to be taken into consideration, which are introduced below.

Involvement of all stakeholders with decision-making power
The structural protection of public spaces only works in the context of an early, interdepartmental co-operation of many players. Clear responsibilities should be defined at the outset.

Planning and Assessment
One such example is the protection of public spaces against hostile vehicle rammings. If such places are analysed generally with a classic concept for vehicle access control, this would inevitably yield results that involve very extensive construction measures, considerable costs, and severe usage restrictions. Whether this is reasonable and wanted in case of an abstract threat posed by terrorist attacks is a matter that should be settled unambiguously in advance. It is therefore strongly recommended to clearly define safety goals before awarding a contract. In this context, it is also highly relevant, whether particular protection is needed permanently or only for specific events.

Prioritisation of security measures
For the protection of public spaces, the situation at the location must first be recorded. Looking back at past attacks, the expertise but also the imagination of terrorists, threat scenarios can be abstracted which can be used to develop measures. The systematic approach of risk analysis is presented in chapter 2.

Clarification of initial financing and ongoing finance
For financial reasons alone, security measures for the protection of public spaces should ideally always be linked to other measures, unless they just involve the placement of a few bollards. Against the background of general and political acceptance, multifunctional measures that serve to improve the urban climate and the urban life quality at the same time also have better chances of being implemented.

The joint search for a compromise
The protection of public spaces against terrorist attacks is only possible by means of compromise. On the one hand, security planning often collides with other interests, processes, needs, and principles. Therefore, potential usage conflicts should be included into the plans from the outset. On the other hand, there are no statutory provisions that contain a defined procedure or minimum standards for protection against attacks, nor are there sanctions in case of insufficient security.

The decision if, how and to what extent a public space is secured against different forms of attack is primarily up to the urban development authorities. Nevertheless, the decision about the implementation of security measures should always rest on several shoulders.

It must be emphasised that public spaces are not at risk per se and should not be treated accordingly. Doing things for the sake of doing them or even fatalism will not help. After all, the planners of public spaces have not just a joint responsibility for the security of the people, but also for a sensible use of taxes and for maintaining a liveable inner-city area.
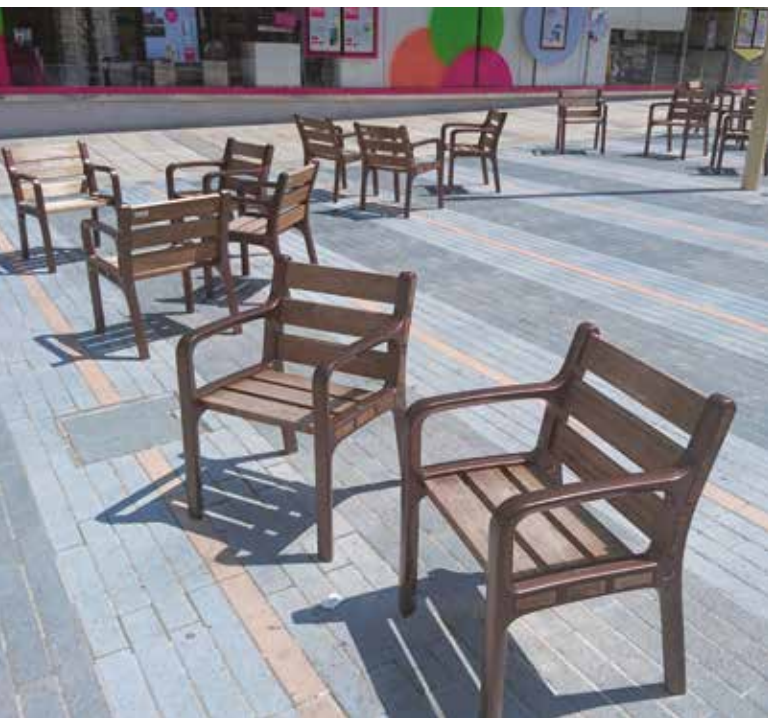
Hostile vehicle rammings – the greatest challenge at present

There is no doubt about the imminent threat posed by hostile vehicle rammings. However, in recent years they played no major role in worldwide attacks. Even in countries with permanent threats of attacks, pure hostile vehicle rammings are rather rare. It is also hardly possible to draw conclusions about a particularly dangerous vehicle mass, a particularly risky attack speed or a particularly dangerous method. It is often other factors that are decisive for the impact, such as the situation, the competence or incompetence of the attacker, the victims' reactions and certainly also lucky or unlucky circumstances. While the vulnerability of public spaces for hostile vehicle rammings can certainly be determined explicitly by means of a risk analysis, the decision about implementing permanent measures is more a political one.

The most significant characteristic of hostile vehicle rammings is that, unlike other forms of attack, they can be prevented fairly efficiently or at least hampered significantly through appropriate barricades.

Good Practice | Austria

Task Force Vienna

In 2008, Vienna started considering how to secure the government district. Based on this, the State Police Division (LPD Vienna) and the municipal executive of the city of Vienna established the task force "Procedure to minimise the risk of hostile vehicle rammings with multi-track vehicles".

Aimed at: Executives from different departments and groups

Objective: Minimising the risk of hostile vehicle rammings with multi-track vehicles in public spaces. Structured, decentralised assessment and implementation of necessary security measures.

Method: Together, a strategy paper for the development of a standardised process was agreed that would identify urgent needs for action and define and evaluate measures:

Level 1: Assessment of a threat situation

Level 2: Specification of the necessary protection level

Level 3: Definition of the protection level to be achieved

The measures should be effective, suitable for everyday use, blend in with the cityscape, and increase the citizens' subjective sense of security. In the end, immediate top-priority measures at Kärntner Straße, Rathausplatz and Mariahilfer Straße were decided on, which have either been implemented already or are in the process of being implemented. The LPD Vienna will be included in future new designs or redesigns. The close co-operation between LPD and the administration of the municipal executive resulted in a concept that focusses on neuralgic points and represents a compromise between suitability for everyday use, compatibility with the cityscape, and effectiveness.

Good Practice | Belgium

Boulevard Anspach in Brussels

In order to bundle authorities and competence, Belgium established the public interest body "Brussels Prevention & Security". It combines federal and regional law and the corresponding competence. BPS acts as a co-ordinator for different stakeholders in the area of prevention and security.

Aimed at: Police, administration, and political decision-makers

Objective: Protection of Boulevard Anspach as part of one of Europe's largest pedestrian precincts. To ensure better co-operation between different players and stakeholders. Better public image of prevention and security issues.

Method: BPS, which reports to the prime minister, tries to reflect as broad a spectrum as possible for matters of security. BPS develops security and prevention plans, tests these and takes charge of their implementation. Even though BPS only has an advisory function, this approach can be considered very effective.

Recommendations

To be able to look at a space and all its aspects, experience and pooled expertise are required. This requires international and interdisciplinary platforms. The structural design of public spaces is exclusively for the future, not for the present or the past.

Thus, models like Boulevard Anspach in Brussels can definitely serve as Best-Practice examples, even without any particular structural measures against terrorism.

Many countries are still searching for perfect solutions – in a space that was never designed for maximum security but instead for maximum of freedom.

→ **Security vs. Aesthetics:** In addition to security, the attraction of a location and the people's feeling of freedom have to be taken into account. There is no absolute security.

→ **Focus on protection against attacks:** The portfolio of crime prevention through environmental design should be further extended and plans for the protection against terrorist attacks be made a firm element in the overall assessment.

→ **Standardised approach:** An early involvement of all stakeholders and continuous co-operation of the different players are essential.

→ **Communication between experts and continuous development:** New jobs for experts as well as opportunities for education and training must be established.

→ **In perspective:** All measures should be applied with as much vision as possible. This applies in particular during periods with increased willingness to invest in light of current events.

> Terrorism does not stop at national borders. It is our duty as police officers to do everything in our power to ensure public safety in close co-operation with authorities and partners. A project like SafeCi gives us the opportunity to set quality standards, learn from Best-Practice examples of others and to improve ourselves as much as possible.
>
> The safety and security of a city can only be ensured by means of well-developed networks.

Michel Goovaerts, Chief of Police Brussels – Capital Ixelles

Belgium

4 Event Security in Public Spaces

Introduction

In large European cities, thousands of people attend events in public spaces each year. Such events are a sign of a free, open, and democratic society and essential for interaction and integration. At the same time, they are attractive targets for attacks because they are heavily frequented, good publicity, and representative. The attackers hope for as many victims as possible.

The security planning process is challenging and complex. Fixed structural protective measures must be supplemented by temporary measures by the police. Ensuring the security of events requires intensive co-operation between the police, organisers, authorising agencies and other security authorities.

Challenges

Which aspects have to be taken into account when planning event security? Events are subject to permission by authorities. First and foremost, security precautions for events must be taken by the organisers themselves.

However, quite frequently additional measures have to be taken by the competent security authorities or the police. Operational planning involves the assessment of all available information. The resulting comprehensive overview of the situation provides the basis for conditions imposed by authorities and for operational measures.

The following explanations provide stimuli for preventive measures and future operational planning.

Reconnaissance measures in the run-up to events serve to gather information about people, groups, organisations, objects, spaces as well as incidents or events and developments in the operational area. They are crucial for the overview of the situation and police tactics. Furthermore, perpetrators often conduct hostile reconnaissance of sites of attacks in preparation of terrorist attacks.

Good Practice | United Kingdom

Project Servator

In the United Kingdom, special reconnaissance measures take place before and during an event.

Aimed at: police officers, general public.

Objective: Identification and disruption of reconnaissance measures of criminals or terrorists; creating trust in the police among the passers-by/the general public; increasing the safety and security of everyone; detecting petty crime.

Method: Police officers receive special training to spot tell-tale signs that someone is planning or preparing to commit a criminal or terrorist act. Uniformed and plain-clothes officers are deployed at irregular intervals and randomly at fixed locations and during events. High visibility is intentional. Passers-by are engaged in informal conversations, while police officers look out for unusual activity in the immediate vicinity. If necessary, they can conduct further investigations. To encourage people to support the police, the psychological mechanism of reciprocity is used.

This conveys that threats can only be countered together. Reassuring communication builds up trust and increases the willingness to report suspicious observations to the police. The measures are flanked by media campaigns.

Crash Test: Concrete Barriers

In a crash test at the DEKRA test site in Neumünster in 2017, two 10-ton trucks drove against several concrete barriers at a speed of 55 km/h, first at a 90-degree angle and in the second test at a 30-degree angle. The barriers had a size of 1.6 x 0.8 x 0.8 metres and weighed approximately 2.5 tons.

The result:

- At an impact angle of 90 degrees, the trucks were able to coast down at high speed without a change of direction. The vehicle was no longer manoeuvrable, but could presumably still move forwards. The driver's cabin was largely intact.
- At an impact angle of 30 degrees, the rear axle could presumably still move forwards. The driver's cabin suffered more damage than at the impact at 90 degrees.
- After 25 metres, both trucks crashed at high residual speed against the impact block (at 90 degrees impact) or the prefabricated wall respectively, which had been set up for secu-

rity reasons (at 30 degrees impact) and were not part of the test.
- Within this area, very severe injuries are likely. Due to the high residual speed of both trucks, people in the immediate vicinity could also have suffered serious injuries.
- Owing to the displacement of the concrete barriers a subsequent vehicle may also penetrate the area at risk unhindered.

Mobile Barriers against Hostile Vehicle Rammings

Events in public spaces are particularly vulnerable to hostile vehicle rammings. For this reason, it is necessary to use mobile and flexible barriers.

In the past, they were often deployed without any experience. Currently numerous findings on the protective effects of mobile vehicle barriers are available due to certification procedures and associated crash tests. It is advisable to have a number of different barrier systems available. The purpose of application determines the selection of barrier systems.

Pros

Use of vehicles:
Vehicles can be moved immediately and thus offer maximum mobility (e.g. for an evacuation of the event area).

Use of concrete barriers:
Unsecured concrete barriers are usually quickly available and economical. A sufficient collision avoidance distance behind the barriers is essential.

Use of wedge barriers:
Wedge barriers are easy to erect and assemble. Due to their low weight, they can be moved quickly, affording authorised persons quick passage to the operational area. A quick evacuation is possible.

Use of water-filled barriers:
The inexpensive foldable containers have a low empty weight and a high capacity. Just a few water-filled barriers can achieve a high blocking effect. They can be set up on any level ground and can also be used for other purposes.

Certification of barriers:
Ideally, only certified vehicle security barriers should be used in future. The German Police University (DH-Pol) in Münster has drawn up an exemplary technical guideline for mobile vehicle security barriers (cf. "Good Practices").

Cons

The actual protective effect of most vehicles (depending on weight and type) is not known.

As crash tests with trucks have revealed, the barriers do not offer sufficient protection at certain impact angles. The barriers themselves can become a danger.

To achieve a high blocking effect, several elements of the costly wedge barrier systems are needed.

They cannot be set up in locations with a strong gradient. In case of an evacuation their removal may take too long. Tamper-proof?

Certification is time-consuming and costly.

Good Practice | Germany

Technical Guideline - Barriers

In 2018, the German Police University in Münster drew up a technical guideline for mobile vehicle security barriers.

Aimed at: Police officers

Objective: Standardise the use of vehicle security barriers and provide a basis for procurements.

Method: The guideline distinguishes between general and specific requirements. General requirements relate to the following criteria:

- Use – Mobile vehicle security barriers must be as simple as possible in technical terms, require little personnel and training, be modular and suitable for flexible use.

- Modularity – Offer the option of a modular construction; quick erection, assembly and disassembly without special technical knowledge.

- Tamper-proof – Manipulation with commercially available means must be ruled out.

- Measures, weights, functionality – Loading, transport, placement and relocation should not require complex infrastructure.

- Weathering resistance – The protective properties of the mobile vehicle security barriers must be ensured irrespective of external conditions.

- Passive safety – Must be constructed in such a way that they do not endanger people and that injuries are avoided.

- Escape routes and evacuation – In case of an incident it is important that escape routes and access for emergency vehicles can be set up quickly and with simple means.

- Maintenance, storage, environmental compatibility – Barriers must be robust and low-maintenance.

Specific requirements describe in particular the concrete examination process: The barriers must be tested at two different angles (45 and 90 degrees). During the test, their effectiveness must be proven. In addition, the performance parameters of a barrier are to be determined for a particular protection class.

Good Practice | United Kingdom

National Vehicle Threat Mitigation Unit (NVTMU)

The National Vehicle Threat Mitigation Unit (NVTMU) is a police unit within the National Counter Terrorism Security Office (NaCTSO) of the British police. It consists of police officers specially trained for hostile vehicle rammings. They are experts in the use of the National Barrier Asset (NBA), a substantial collection of certified mobile barriers.

Aimed at: Police officers of the NVTMU, co-operation partners from other authorities, politics and industry

Objective: Bundling competences and equipment related to hostile vehicle rammings. Identification of innovations and setting new standards for mobile barriers.

Method: The NVTMU works closely with the Centre for Protection of National Infrastructure (CPNI). It helps with risk assessments, provides tactical advice on hostile vehicle rammings and provides mobile barriers, if needed. It is the interface between police, other authorities, and politics on the matter of threats posed by hostile vehicle rammings. Support is also provided by industry, in particular when additional barrier systems have to be transported or hired for large events. NVTMU staff work across the entire United Kingdom and will also travel overseas, if necessary.

Recommendations

For event security in public spaces, bundling knowledge (know-how and technology) is essential. By involving the general public and accompanying police measures, a comprehensive picture can be obtained to assess the situation.

Basic requirements for the protection of public spaces:

→ **Cooperation between all parties involved: This is the key to a safe and secure event – based on a diligently planned security concept.**

→ **Bundling knowledge:** A central point of contact should have expertise in terrorist attacks. Bundling knowledge is also advisable in the complex field of mobile vehicle security barriers, in particular when non-certified systems are used.

→ **Use of certified systems** There is no such thing as the perfect barrier – depending on local conditions, each system has its advantages and disadvantages. It is important to carefully consider which certified systems to use. Barriers used incorrectly can become a great risk.

→ **Reconnaissance:** A continuous involvement of the general public, flanked by police measures, has proven to be successful.

Protection of Critical Infrastructure

> We are constantly looking for new ways to secure public spaces and events in our city. This is a job that never ends. And new insights are always fascinating.
>
> The SafeCi project has given us the wonderful opportunity to learn from our European colleagues. At the same time, we were able to explore new avenues to make our cities safer for our citizens as well as for tourists. We are delighted that we were able to contribute to the success and further development of the project by exchanging expertise.
>
> By sharing our experiences with other police authorities of the partner network, we also receive excellent feedback on our own approach to police work.

Erik Widstrand, Chief of Police Stockholm City, Polismyndigheten

Sweden

Introduction

Communication is the essential key factor for quick and reliable decision-making processes in crisis situations and serves to minimise risks in advance.

Critical infrastructures are the lifelines of our modern society. Their complex structure surrounds and permeates the political, economic, social, and cultural centres of our society. A failure or impairment of their functionality has far-reaching consequences for the general public and the respective centre of finance, industry, trade and commerce.

These days, both private and public operators of critical infrastructures are confronted with a variety of risks, from natural disasters or accidents to the increasing number of criminal attacks.

Besides the classic cyber-attacks, new technological developments present gateways for attackers, not least of all for systematic terrorist attacks for years now. In particular for highly-developed industrial nations, the continuous failure-free functionality of critical infrastructure is of fundamental importance.

The responsibility for the identification of critical infrastructures always rests with the state. Private and public stakeholders are involved. This requires a co-ordinated approach and suitable, reliable communication structures.

Critical Infrastructure

Until now, there has not been a standardised, binding definition of the term "critical infrastructure" in the partner countries. According to the EC Council Directive of 8 December 2008, " 'critical infrastructure' means an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions (...)".

A survey among the partner countries revealed that a determination of critical infrastructure was always preceded by the following questions:

+ Is there any mutual dependence of critical infrastructures? (Interdependence)
+ How significant is a critical infrastructure in terms of the consequences of a malfunction or disruption for the security of supply for a society? (Criticality)
+ How can the impact of disruptive events be mitigated, thus guaranteeing the continued provision of the basic functions of a critical infrastructure? (Resilience)
+ How susceptible to damage is a critical infrastructure? (Vulnerability)

Challenges

Communication is the essential key factor for the identification and protection of critical infrastructures. This became clear during the intensive exchange between the project countries.

However, this exchange is not always uncomplicated. Therefore, interdisciplinary teamwork between state actors and private institutions is indispensable.

+ Communication gathers a momentum of its own in the context of public administration and bureaucratic decision-making channels, federal structures, and responsibilities of several authorities in the same subject matter, as well as classic principles of separation under constitutional law.
+ The exchange of information by operators of critical infrastructure is often very restrictive.
+ The framework for communication in crisis management is European. However, most of the project partners are police authorities at state or regional level, whose focus of interest is on adequate concrete police measures.

The Austrian Programme for Critical Infrastructure Protection constitutes a Best-Practice example that is unique by comparison. The identification of critical factors for successful communication between government stakeholders and operators of critical infrastructure should therefore be guided primarily by the approach of the State Police Division Vienna.

Best Practice | Austria

Austrian Program for Critical Infrastructure Protection (APCIP)

The Austrian Programme for Critical Infrastructure Protection (APCIP) is based on the European Programme for Critical Infrastructure Protection (EPCIP).

Aimed at: Austrian authorities and providers of critical infrastructure.

Objective: Increase the resilience of critical infrastructures. The affected businesses are to identify potential vulnerabilities by means of a comprehensive risk analysis. Measures derived from this analysis are intended to avoid, mitigate or prevent risks. In addition, the business continuity management of the businesses or organisations is to be improved and a security management system set up.

Method: In addition to the voluntary co-operation of the stakeholders, the following principles apply:

All Hazards Approach: "Safety risks" (natural hazards, disasters caused by humans, and technical failure) as well as "security risks" (criminal acts, terrorist attacks etc.) are taken into consideration.

Operator-based Approach: For the identification of critical infrastructure, Austria follows the respective operators and fully co-operates with them.

Subsidiarity and Self-commitment: The operators and owners of critical infrastructure are responsible for the protection of their assets and facilities. A voluntary self-commitment and a commitment to increased protection standards are to increase the business' resilience.

Complementarity: Resolutions on new measures or plans to build on existing ones; these are adjusted in accordance with the respective type of threat and threat situations.

Confidentiality: The information exchanged in the context of APCIP is confidential. Information is processed on a "need to know" basis.

Commensurability: The costs and measures for increasing resilience are adjusted individually to the respective risk situation.

Co-operation: An exchange between all stakeholders is intended to further develop APCIP and ensure its efficient and effective implementation. By involving businesses, interest groups, public administration, standardisation institutes and media, different perspectives are taken into account.

The APCIP Programme involves the following key steps:

Initially, the critical infrastructures in Austria are identified and compiled in a list that is updated and amended annually.

A subsequent categorisation then allows for a prioritisation. In terms of the impact of a failure of critical infrastructure, a distinction is made between national and European (at least two member states affected).

Using an assessment matrix, the impact on the respective critical infrastructure in case of a disruption or failure can then be assessed.

Affected companies are then assigned one of three categories (A, B, and R) in co-operation with the operator of the critical infrastructure:

Category A: The life or health of people is affected. At least one criterion in the red area and none in the green area of the matrix.

Category B: At least one criterion in the red or yellow area of the matrix.

Category R: At least one criterion in the red or yellow area of the matrix, but limited to a single state.

| Assessment Matrix for Critical Infrastructure			
Impact	**High**	**Medium**	**Low**
Time	Minutes/hours	Days/weeks	Months/years
Type	Life/health; functioning of the state affected to a high degree	Great economic damage; functioning of the state affected	Low economic damage; other effects
Extent	Large parts of the population (at least 1 %)	Parts of the population (at least 0.1 %)	Individuals
Redundancy	Service not/barely substitutable	Service substitutable for a short period	Service substitutable for a longer period

Recommendations

In summary, communication is the essential key factor for the protection of critical infrastructures. For that purpose, interdisciplinarity at all levels between state actors and private institutions is indispensable. This requires binding structural guidelines.

The protection of critical infrastructures is based on four pillars:

→ **Preparation:** Successful crisis management is only possible if communication is timely, effective, and efficient. Forms of communication must be defined and the parties involved must be familiar with the communications structures of the respective other party. Communication in a crisis must be defined in a communication concept before a crisis occurs.

→ **Extensiveness:** State actors and operators must systematically co-ordinate and network their objectives, processes, and structures as well as their capabilities and resources beforehand.

→ **Confidentiality:** The implementation of effective and suitable protective measures rests with the operators themselves. In particular in practical terms, informal communication channels are essential for a successful co-operation between them and the state actors. In case of a crisis, informal communication across different levels and departments could make all the difference. For that purpose, a basis for trust is imperative.

→ **Transparency:** There is still little awareness among the general public regarding the risks and dangers that critical infrastructures are exposed to. It is advisable to consider how this awareness can be raised and sustained by means of transparency, information, and advice.


TRANSPARENCY · PREPARATION · PECT · CONFIDENTIALITY · EXTENSIVENESS
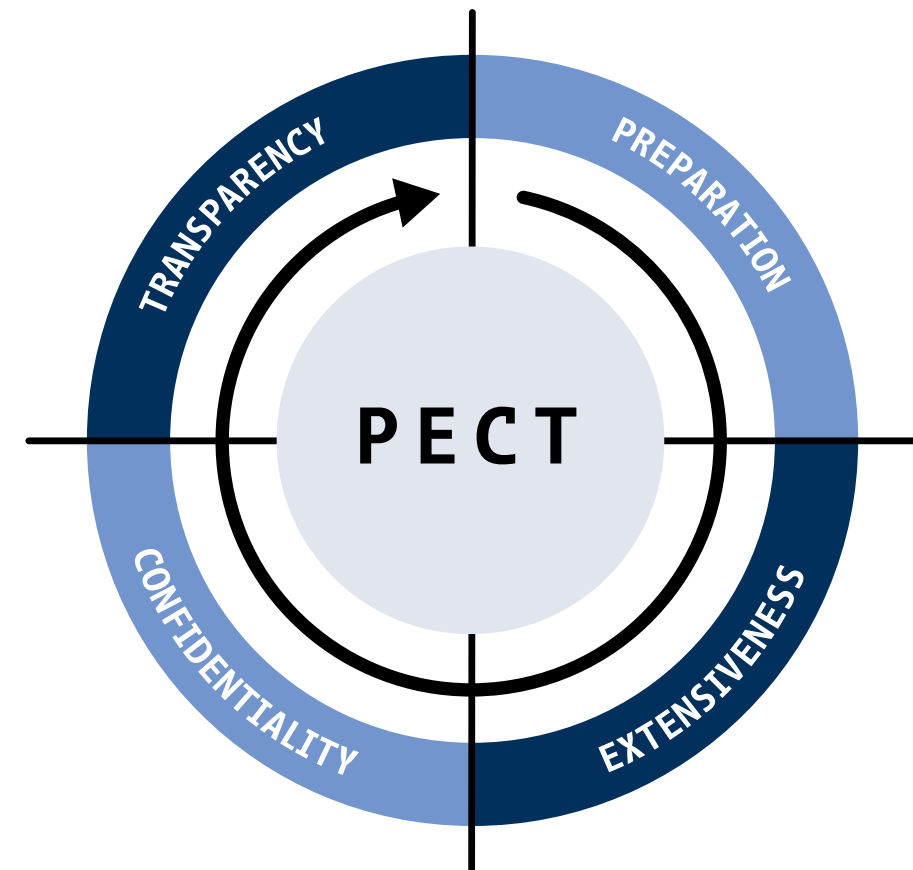
> As the police president of Vienna, I am delighted that the capital of Austria participates in the "SafeCi – Safer Space for Safer Cities" project.
>
> The security of the population has highest priority for us. This successful transnational project has once again proven the importance of international exchange. Only together and in co-operation with different partners can we contribute effectively to preventing terrorist attacks and further extend the protection of the general public.

Dr. Gerhard Pürstl, State Police President, State Police Division Vienna

Austria

6
Innovative Approaches to the Protection of Public Spaces
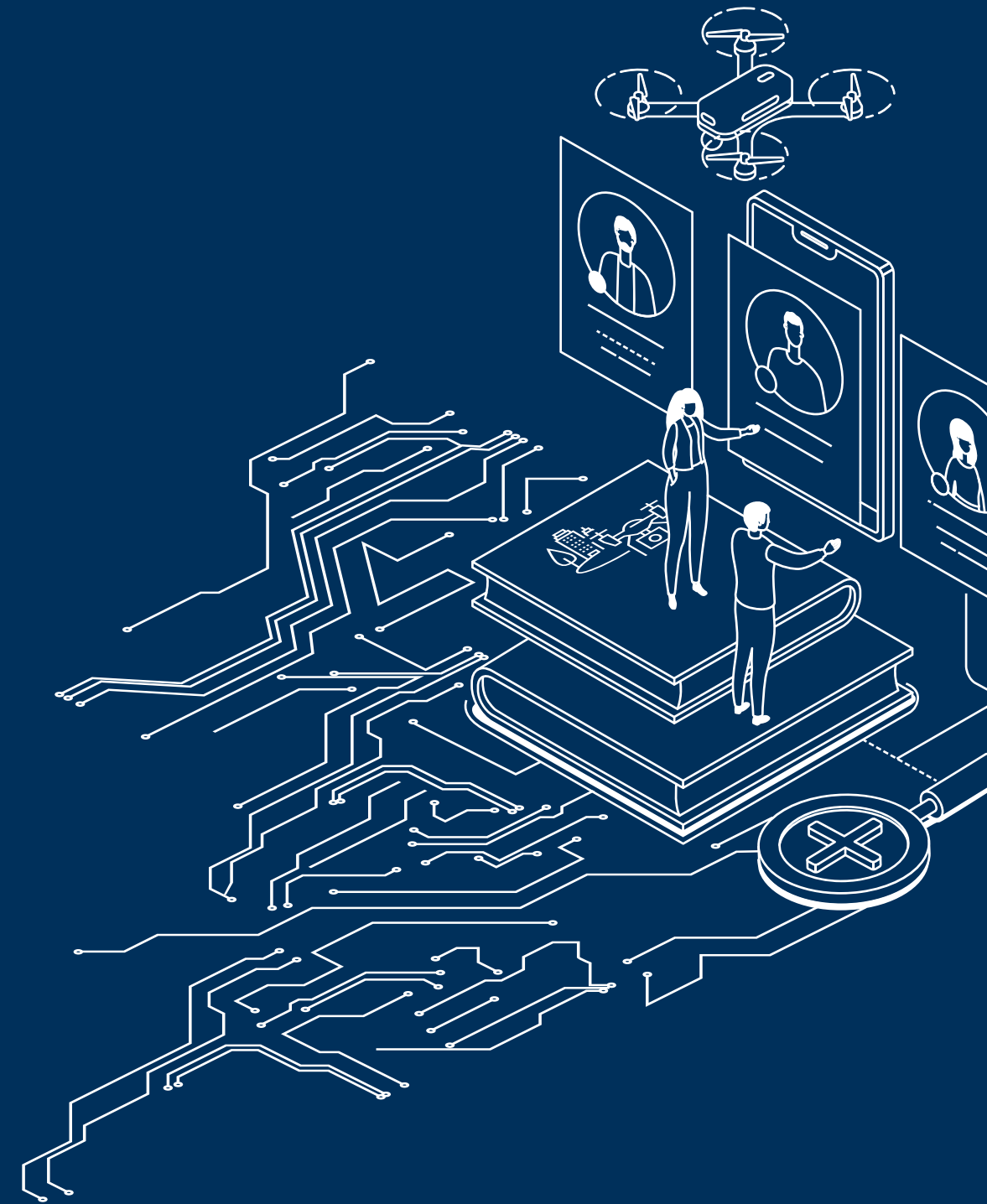
Introduction

When used improperly, the new technologies can present a threat to public spaces that is difficult to assess. It is therefore vital that European security authorities tackle the issue of drone technology. The same applies to new methods for person recognition and video surveillance.

Progress does not stop at the protection of public spaces. Possible solutions undergo continuous development. In addition, new forms of terrorism force security authorities to constantly adapt to changing threat situations. This affects both new trends in the focus of terrorist activities and new forms of attack that were never or hardly ever noticed before.

Thus, changes in the prevailing conditions and the dynamics of technical developments force security authorities to also look at innovative approaches to the protection of public spaces.

The focus here is primarily on drones and perception-based technologies.

Challenges

Drones and the Protection of Public Spaces

During the last decade, Unmanned Aerial Vehicles (UAV) have become part of pioneering technologies. This development can be attributed primarily to the considerable expansion of technical opportunities in recent times and the associated new areas of application for drones.

However, an increased spread of drones also entails threat scenarios for public spaces. It is therefore of utmost importance that the police authorities of European cities look at the issue of drones more closely than before – and at the options for the prevention of and defence against realistic threat scenarios.

In doing so, the following aspects should be taken into consideration:

+ **The concept of drone defence systems is still at an incipient stage, both from a technological and social perspective.** It requires regularly updated assessments of the development processes.
+ **Legal foundations are elementary for measures to protect public spaces.** In the civil drones sector, this affects the regulation of technical requirements and permitted applications as well as the framework conditions for drone operation and use by private users, authorities, and commercial users.
+ **Drones can be used for a variety of police tasks,** make them easier or increase the quality of solving police problems. However, only a part of the possible applications actually falls within the ambit of the protection of public spaces.

+ **The use of drones by the police Is legally controversial.** For the use of UAV by authorities, additional fields of law (police law, data protection law, constitutional law etc.) that go beyond basic regulations are becoming increasingly relevant. In addition, acceptance by the general public and occupational health play a role that should not be underestimated.

It becomes clear that in future the police in Europe should attach greater importance to the issue of drones. This concerns, inter alia, the strategic alignment of police authorities but also the financial and human resources of police units dealing with drone defence systems and the use of drones. The police authorities of the partner countries have reported different framework conditions and facilities. Co-operation and exchange of experiences are essential processes to ensure the police's ability to act at a European level.

Threats to Public Spaces in the Context of Drone Technology

Two aspects in particular should be taken into consideration by police authorities and political decision-makers across Europe:

+ **There is an ever-growing number of drones.** Decreasing prices will also contribute significantly to this development (estimate for the year 2050: approx. 400,000 UAV for use by authorities and for commercial purposes, of which around 50,000 for the work of the police and fire brigade; approx. 7 million drones used privately).

+ **Drones could be used as weapons** by attackers steering them deliberately at individuals or crowds. Their design alone would likely result in serious injuries. In addition, they could also be used as a means of transport for explosives or CBRN substances. Firearms attached to drones could be triggered by remote control. Individual extremist attackers or organisations might gain illegal access to drones and then misuse them.

Police Protection of Public Spaces in the Context of Drone Technology

There are several thematic key aspects related to the use of drones for the protection of urban public spaces

+ **Awareness-raising:** In the context of PR work by the police, awareness-raising in connection with UAV should only affect the police marginally and spontaneously (e.g. providing information to pilots who violate regulations without the intent of endangering anyone). Alternatively, awareness-raising campaigns and raising awareness in the context of consultancy work are conceivable.
+ **Drone defence:** According to prevailing opinions, drone defence consists of three stages: detection, identification/verification, and the actual defence. Therefore, successful drone defence depends on technical, financial, organisational, HR and legal conditions. The technical aspect in particular is subject to continuous development as the technology of drone defence systems must keep up with the rapid development of aerial vehicles.
+ **Use of drones by the police:** Drones can be used in a variety of ways by the police. Some of these application scenarios offer opportunities to increase the protection of public spaces.

+ **Framework conditions:** EU regulations (for the operation, insurance, and specifications of UAV) apply to all member states and can be supplemented or fleshed out at national level. The police adhere to the air traffic regulations of the respective member state. Legal aspects meet with social reservations and doubts – therefore, the issue also touches upon ethical matters.

Perception-based Technologies

Video surveillance and artificial intelligence

The issue of video surveillance by government institutions for the protection of public spaces is emotionally highly charged. For years, it has been the subject of intense discussions both in terms of social policy and data protection.

In times of intense social change or political crises, the general public's desire for safety and security increases. Video surveillance constitutes an important element in the protection of public spaces – to avert danger and to prosecute any offences already committed.

Due to the rather low costs these days, comprehensive video surveillance for the purpose of protecting public spaces usually entails monitoring a large area directly by means of cameras and systems connected with them.

In connection with new technologies and large data volumes, the term "Big Data" is also used frequently. Since video surveillance of public spaces, in particular buildings and large open spaces, involves a large number of cameras, vast amounts of data are produced. Not only must they be secured, but ideally viewed or analysed live.

It is difficult to store vast amounts of data in the long term and to archive them in a way that ensures that they can still be used in a meaningful way at a later stage. A logical next step would be a pre-selection by software programmes that use Artificial Intelligence (AI) to put the video files in a meaningful order for viewing. This method is also subject to legal limitations, as data protection, data security, and data minimisation are considered very heterogeneously within Europe. In general, the use of systems based on artificial intelligence can significantly reduce human effort for viewing video footage.

Surveillance

According to David Lyon, a leading researcher in the field of surveillance studies, surveillance is the "focused, systematic and routine attention (...)". It is usually intentional and involves the use of certain protocols and techniques. "Classic" video surveillance records an incident or event randomly or spontaneously. The material is then viewed later for the purpose of analysis.

Super Recogniser (SR)

The term "Super Recogniser" has been used differently by the media, by law enforcement practitioners, and by scientists. Even within each of these fields, there is no consensus about the meaning of the term. In the context of this manual, the term denotes people with a naturally occurring, exceptional ability to recognise and process human faces.

Super Recognisers in policing

In recent years, international security authorities have become increasingly interested in Super Recognisers (SR). Due to their special skills, SR could help to detect threats to public spaces – and thus save lives. In Germany, several state police authorities have independently taken steps to identify and/or deploy such SR.

Special challenges:

+ There is no generally accepted definition of the term.
+ It appears questionable whether the professional expectations towards SR (provided they are clearly defined a priori) can be met.
+ To date, there are no empirically validated, appropriate, commonly accepted criteria/tools for the selection of SR in police authorities.
+ There is no systematic approach to collate and communicate findings in order to evaluate measures for the selection and deployment (of SR). This is crucial in order to evaluate the appropriateness and the benefits of using SR for future operational strategies of the police and thus comply with the requirement of evidence-based police work.

Humans can process faces at increasing levels of complexity. In addition to visual perception, recognition and identification as the top levels of processing also rely on memory. All levels can be affected by image variations – for example by age-related changes or differences in illumination or image resolution.

Deployment areas for SR:

+ **Investigations of terrorist attacks** and further crimes or preventative operations to mitigate threats.
+ **Analysis of pictures and videos** from surveillance technology in order to identify suspects and/or victims or to verify hits provided by face recognition software.
+ **Avert threats to public spaces** – for example when the police receive intelligence about a planned attack on a public space. In this case, SR could detect attackers and pave the way for follow-up measures.

Good Practice | Germany

Berlin Test for Super-Recognizer Identification (BeSuRe)

Since 2017, the Innovation Management unit of the Berlin CID has been co-operating with scientific partners under the direction of Dr. Meike Ramon of the University of Fribourg (Switzerland), a leading expert in the field of the human ability to recognise and process faces. Together, they have developed a test procedure, the Berlin Model for Super Recogniser Identification.

Aimed at: Berlin CID (Innovation Management), police officers, research

Objective: Bridging the gap between scientific findings and their practical application. Identification of "Super Recogniser" types.

Method: Development of a test procedure that was specifically tailored to the concrete interests and needs of the Berlin Police. It consists of two stages in which scientific state-of-the-art procedures are combined with materials and scenarios relevant to police work.

- An initial test serves to identify people with below-average face processing skills. Thus, these people can be excluded from the overall pool.
- The remaining people can take part in further tests for which authentic police photos and video material are used. Various scenarios are simulated that SR would have to handle during a real operation. The various conditions reproduced this way allow for a more differentiated distinction between the performance profiles of the test persons (their hit rate and response time in different operational scenarios). This is useful for their subsequent skill-based deployment.

In the autumn of 2020, the pilot phase of the BeSuRe was launched. Afterwards, approximately 18,000 police officers, can take part voluntarily. Once validated, it is planned to make the BeSuRe available to other police authorities, too.

Good Practice | Finland

Drones: Finnish Police Unmanned Aviation

Since 2012, the Finnish police have been looking closely at the use of drones to support police work. The UAS Task Force of the Ministry of the Interior drew up essential steps early on. Since 2014, these steps have been implemented gradually by a co-operation group within the Ministry of the Interior.

Aimed at: UAS task force and co-operation group at the Ministry of the Interior, police officers

Objective: Overall increase in the efficiency, effectiveness, and occupational safety of police work involving the use of drones and drone defence systems.

Method: In Finland, over 160 UAS are now used by the police (consumer models, professional models built in Finland, specifically tailored to the requirements of the police).

- Following the preparation of an RPA/S directive for the police and the procurement of UAS, intensive training has taken place since 2017.
- In 2019, the Finnish police already had more than 390 trained drone pilots (over five percent of all police officers in Finland, of which 40 in Helsinki alone).
- More personnel is trained continuously. Further training programmes to acquire tactical skills for the use of UAS were developed.
- An expert task force for the misuse of UAS, established in 2018, has also addressed the development of drone defence concepts.
- In 2019, the Finnish police also started procuring, testing and using detection and disruption technology.

In addition to monitoring events, UAS are used for close protection, crime scene investigation, reconnaissance, observation, the search for missing persons, obtaining information for police operations, and for searches.

Good Practice | Sweden

Video Surveillance – Stockholm

The city centre of Stockholm is exemplary for increasing the security of public spaces by means of well-planned and extensive video surveillance by the police:

Aimed at: Police, private players

Objective: Increasing the security of public spaces.

Method: Many public spaces in Stockholm (such as shopping centres, train stations, and smaller shops) are monitored by means of camera technology. This is operated privately. For the underground network, the private operator also retains personnel for a real-time analysis.

- If anything unusual is noticed, the police send out officers in cases of suspicious circumstances.
- For special occasions, additional rights may be activated for the police, thus allowing them for example to view certain cameras or video surveillance measures in real time.
- The police have also installed cameras in public spaces and conduct video surveillance measures. The police authority decides which places are classified as hotspots and how camera technology

is installed on the basis of existing laws. They cover the costs themselves and use their own means and resources to install the cameras. The city of Stockholm provides electricity and network capacity.

- Police cameras installed in the city centre, which cover the places most often affected by crime, are looked after, monitored, and analysed in the police command centre.
- Police officers can also view the video footage directly on site and respond quickly.
- All police cameras are very high quality and offer the option of a live link-up.
- Due to recent changes in Swedish legislation, it has become possible to use video footage even retrospectively for criminal prosecution.
- Future plans for the Stockholm police include a comprehensive camera surveillance centre in which police officers view the cameras live and operate them.
- Additional camera systems of private operators are to be integrated into the existing system.

Good Practice | Israel

Video Surveillance – Jerusalem

The Israeli police come under the control of the Ministry of Public Security. They have approximately 30,000 police officers and around 45,000 civilian auxiliary staff. The police alone are responsible for police work and criminal prosecution in Israel. Jerusalem's old city has 35,000 residents and is visited by many tourists from all over the world. Due to its political relevance and strong tensions between the religions, Jerusalem is the centre of permanent conflicts.

Aimed at: The Mabat 2000 unit of the Israeli police, which is responsible for video surveillance in Jerusalem's old city.

Objective: Prevent attacks before they happen; identify attackers if an attack cannot be prevented; transmit real-time reports to the police officers on site.

Method: In the police command centre, images from more than 400 cameras are collated in real time and even offer 360-degree footage. According to Mabat 2000, this technology is among the most advanced of its kind anywhere in the world.

- Specially trained police officers monitor the situation on screens and work in shifts 24/7.
- They view and examine correspondence with the nearby secret intelligence service for potential threats.
- In addition, they constantly monitor the situation in Jerusalem's old city. Even during their training, they learn to identify all streets and alleys and which cameras can show which angles.
- On top of that, more than 600 officers patrol Jerusalem's old city on foot. They constantly communicate directly with the command centre.
- The system allows for a retrograde viewing of recorded sequences and therefore a precise determination of where attacks took place. If a suspect is arrested, his/her face is recorded on video, behind closed doors, as evidence for the court.
- With their stationary camera systems, the police can also trace offenders in real time, even if they escape into a building or change their clothes. In Israel, such recordings are valued very highly in court proceedings. They can be used as evidence.

Recommendations

As part of the SafeCi project, drones were identified as one of the currently most relevant technologies in connection with the protection of public spaces. In the long term, it appears inevitable that European police authorities will look closely at the issue of drones, thus making sure they are equipped for the future. Video surveillance also plays an important role in the protection of public spaces. In addition, it can prevent politically motivated crimes such as terrorist attacks or allow for immediate intervention.

Furthermore, Super Recognisers can support the work of the police significantly. However, before they are deployed routinely, we need a better understanding of their unique skills.

Prerequisites for the Use of Innovative Technologies in the Protection of Public Spaces:

→ **Continuous exchange of ideas:** It is crucial that SafeCi project partners and further potential partners continue to transfer insights and "Good Practices" on the issue of innovative technologies and in particular drones – especially in the context of technical advances and new manifestations of terrorism.

→ **Establishment of a drone budget:** Police authorities should set a budget for the use of drones, thus enabling them to make long-term strategic plans without burdening other sections of the police with additional costs.

→ **Use of face recognition software:** When designing video surveillance concepts for public spaces, it is advisable to implement face recognition software based on AI.

→ **Sound approach to the selection and deployment of SR:** We need a better, scientifically-based understanding of the unique skills of Super Recognisers and an evaluation of the effectiveness of their deployment compared to traditional methods of police work.

Awareness-raising Strategies for the Protection of Public Spaces
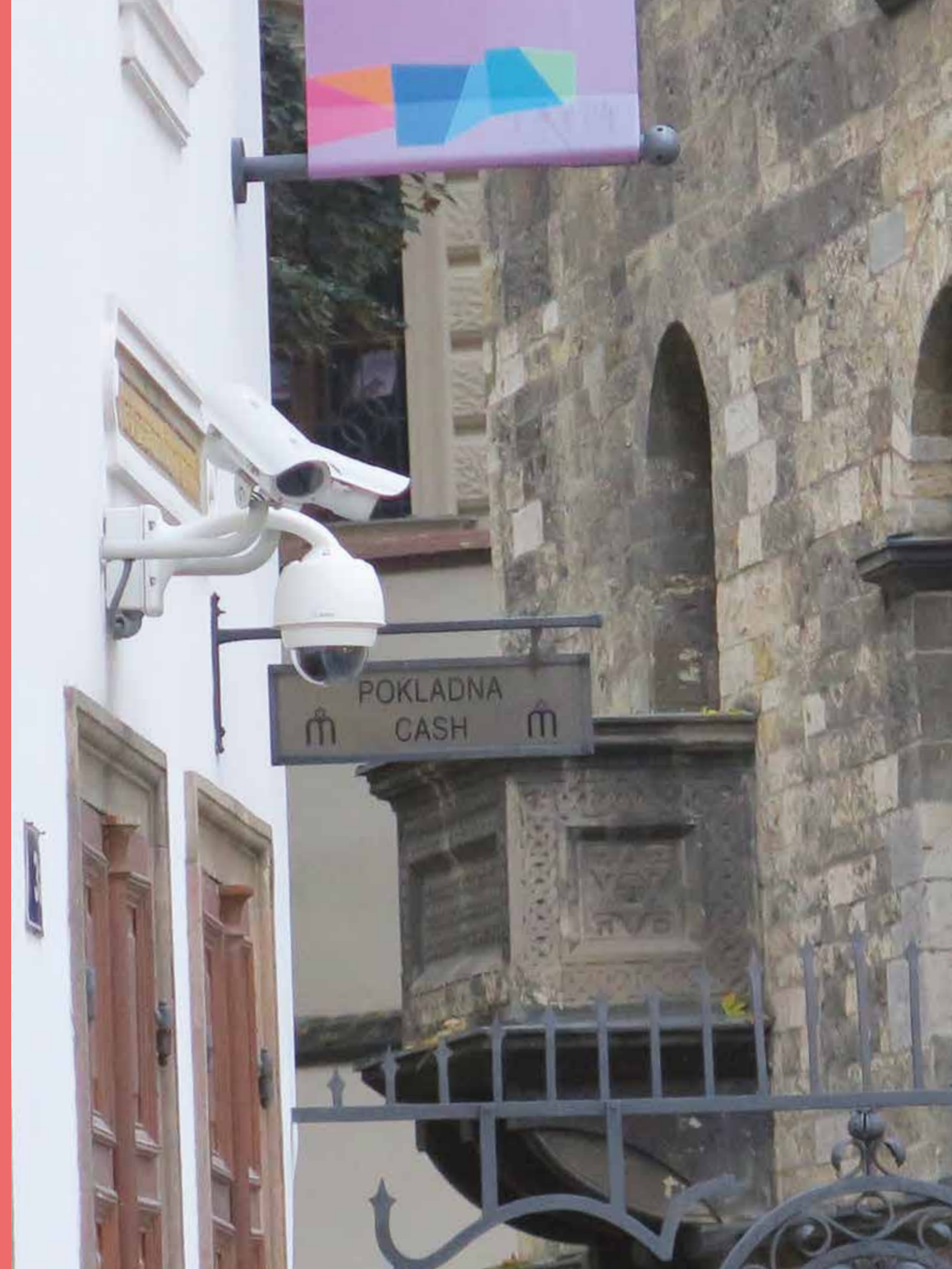
> If we want to protect our cities, we should exchange tried and tested practices and technologies.
>
> Sharing insights we have gained and Good Practices at local, national, and international levels allows us to identify weaknesses, mitigate risks, and make Helsinki a safer city. SafeCi is a successful example of international co-operation aimed at increasing everyone's safety and security.

Lasse Aapio, Chief of Police of Helsingin poliisilaitos

Finland

Introduction

In particular with regard to terrorist at-tacks it becomes clear that the communi-cation and information required for long-term awareness should always be part of a comprehensive communication strategy.

Most of us are familiar with awareness-raising strat-egies for a variety of threats that might have a direct influence on safety and security in public spaces. Ex-amples in case are safety instructions on airplanes, announcements regarding unattended luggage, fire drills or advice on how to handle dangerous diseases like the Corona virus.

Raising awareness in terms of terrorist crimes is a very demanding task, not least of all due to the numerous forms of attack. Raising awareness for all possible kinds of attack would not just overwhelm most people but probably result in uncertainty and rejection.

It is also not easy to define the relevant content: focussing on too much is quickly condemned as scare-mongering, while a hesitant disclosure of information quickly results in an accusation of irresponsibility. Especially in life-threatening situations, people tend to overreact emotionally. This must be taken into consideration. If possible, accessible, simple, and true-to-life advice should be compiled that will be widely accepted.

With this in mind, the consideration of awareness-raising strategies in the context of the SafeCi project will deal with different forms of com-munication and discuss how to embed these in a holistic communication strategy.

A directive (EU 2018/1972 **EECC**) of the European Parliament and of the Council obliges the EU member states to implement technical solutions to comprehensively warn the population by the year 2022.

Awareness-raising Strategy

A multi-layered, methodical, and systematic approach to influence the reaction of people to certain situa-tions. It is based on two main pillars: efficient communication and targeted information. It covers both the acute moment of a threat and the time periods beforehand and afterwards.

Challenges

An effective strategy comprising risk and crisis communication provides the basis for long-term awareness among the general public about how to handle life-threatening situations.

Risk communication:

+ Mainly prevention: building up systematic awareness of threats
+ Addressing the issue openly, transparently, and credibly
+ Practical and theoretical information
+ Establishing a basis for trust and communication
+ Prerequisite for successful crisis communication

Crisis communication:

+ Essentially damage limitation: increasing the chances of maintaining control over public opinion and interpretation in case of an attack and of preventing speculation and panic.
+ Basic principles: promptness (active, early), truthfulness (objective, transparent, true), comprehensibility (brief, simple, straightforward, graphic), and consistency (uniform, co-ordinated, continuous) (Source: BMI 2014).

It is crucial that the individual perception of citizens meets with a uniform, objective, and problem-oriented police strategy that does not give rise to a feeling of uncertainty, overwhelm people or appear irrelevant.

Developing a strategy

An overall concept of raising awareness – which goes beyond individual measures – should be suitable to detect preparations for attacks more quickly through clear safety regulations and increased awareness and to respond in a timely manner. The advantage of such a concept: once established, the forms of communication can be extended, amended or renewed repeatedly, without having to reinvent the wheel every time.

For the successful implementation of an awareness-raising strategy, five levels are crucial: objective, target group, content, medium, and period of time. Who is to be reached, in what way, with which content, at what point in time and what objective is pursued with this?

One tool to analyse such a strategy beforehand is a business tool called SWOT analysis. It provides a simplified illustration of the strengths, weaknesses, opportunities and threats of an action.

SWOT analysis using the example of luggage information at airports and train stations

Strengths
- Target group can be reached easily, numerous channels available, clear reference to potential, prompt sanctions for misconduct, simple efficiency control.

Weaknesses
- Language barriers for travellers, possible habituation effect, lack of attention among stressed travellers.

Opportunities
- Changing awareness in terms of own luggage and third-party luggage, lightening the load of security officers and operational staff, reducing chances of successful attacks with suitcase bombs and pickpocketing.

Threats
- Raising too much awareness could result in increased nervousness and overreactions, more reports of even minor offences, and a greater burden on security officers due to an increased case load.

Selection of suitable measures

On the one hand, preventive measures must move with the times, on the other hand they must still use classic channels. Each communication and each information has its target group and time window.

Potential measures and channels:

- Police advice on preventing terrorist attacks
- Flyers and brochures
- Outdoor advertising using posters, placards, and advertising boards
- Internet campaigns – information material
- Short films and trailers
- Upload pages/Dark pages
- Social media
- E-Learning offers
- Location-based services

Apps also offer numerous options for awareness-raising measures and communication before, during or after a terrorist attack:

- Warning apps
- Emergency services apps
- Police apps
- Messenger apps

There is probably no universal and verifiably successful strategy to raise awareness among the general public about life-threatening threats such as terrorist attacks. Numerous influencing factors such as the willingness of people to take information by the police seriously, the individual habits of using media, and the current threat situation have a crucial influence on the success or failure of communication measures.

	Awareness-raising strategies Communication – Information				
Category	**Risk communication**	**Crisis communication**			
Channel	Police advice	Location based SMS		Police advice	
		Emergency services apps	Cell broadcast	Flyers, brochures	Upload platforms
	E-learning offers	Dark pages			
	Short films & teaser	Internal messengers			
	Flyers, posters, brochures	Warning apps			
	Public advertising boards				
	Information websites				
	Radio, TV, magazines				
	Police apps				
	Social media				
Time axis	**Before an attack** Awareness-raising, information, prevention	**During an attack** Warnings, advice, information		**After an attack** Damage limitation, support, information	

Good Practice | Luxembourg

Citizen Cop

The function "Citizen Cop" is part of a comprehensive app of the Luxembourg police with the slogan "The Police in your Pocket".

Aimed at: General public

Objective: Timely co-operation (gathering information and evidence)

Method: Users can report suspicious circumstances in a timely, simple and unfiltered manner, thus avoiding the typical "suppression effect" which often occurs when there is a time delay before a report can be made.

- Images and texts can be sent directly to the police at the click of a button.
- The app is not completely anonymous (prior registration with name, e-mail and telephone number is necessary).
- Information can be processed professionally.
- Additionally, the app offers options for push notifications to send appeals to the general public and to deny rumours in threat situations.

Good Practice | Austria | Germany
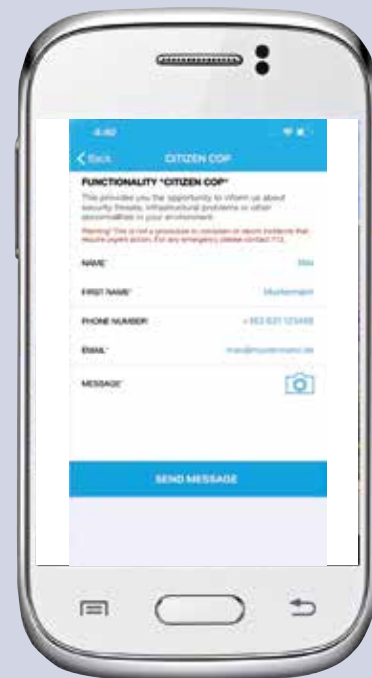
KATWARN

KATWARN was developed by the Fraunhofer Institute for Open Communication Systems (FOKUS) on behalf of the German public insurance companies. It has been available since 2011.

Aimed at: General public (in case of danger)

Objective: Alarm, warn, instruct, support

Method: The app offers short, brief information on threat situations as well as recommended actions directly and during a threat situation. It sends official warnings to users via push notifications.

- KATWARN is also linked to the Modular Warning System (MoWaS) of the German Federal Office of Civil Protection and Disaster Assistance and the German Meteorological Service.
- Warnings can be received for the current location and/or for seven selected locations. In addition, a map of the affected location is shown.
- Warnings can be shared directly from the app via social media and other apps installed.
- Users can subscribe to topics (e.g. selected occasions or large events). This function is still under development (currently only available on the website and on hessenWARN).

- KATWARN can also be used in-house by companies and other institutions to warn their customers and employees.
- Based on the KATWARN technology, the KATRETTER app was developed for first aid volunteers.
- Even when abroad, roaming technology allows the users to receive warnings for their current location if this country, such as Austria, also uses the KATWARN system.
- The EU Commission uses the international warning system EUWARN to warn its employees. EUWARN is based on KATWARN.
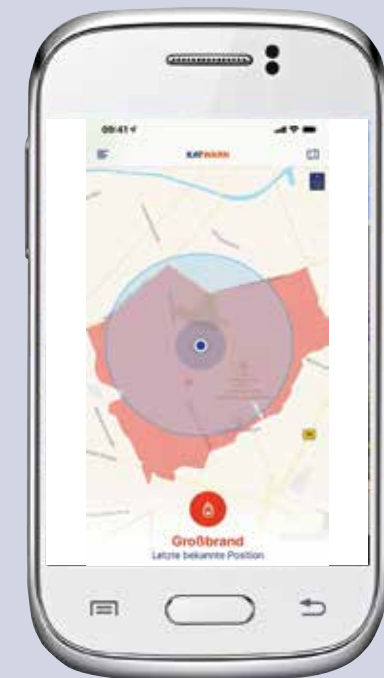
Good Practice | Sweden

If crisis or war comes

The Swedish Civil Contingencies Agency (MSB) has compiled a 20-page brochure entitled "If crisis or war comes".

Aimed at: General public

Objective: Preparation for crises

Method: The brochure was sent out to all households in Sweden. However, it is important to keep in mind that this brochure has been published in Sweden for a long time – in other European countries, a brochure with such a title being sent to all households might give rise to misunderstandings.

- It contains advice on how to behave in case of a crisis such as a terrorist attack, in the event of Sweden having to defend itself or in case of a failure of essential supply capacity. In addition, it contains important phone numbers in case of emergency, information on national crisis management and ways to prepare individually for a crisis.
- Offers useful advice and makes people aware that we still live in an unsafe world.

Good Practice | United Kingdom

The ACT campaign of NaCTSO

As part of its ACT campaign (Action Counters Terrorism), the National Counter Terrorism Security Office (NaCTSO) in the United Kingdom has published a variety of information on how to behave in situations involving serious violence.

Aimed at: Primarily employees of institutions and facilities with a high number of visitors (such as shopping centres, football stadiums, event locations, religious institutions, schools).

Objective: Information, prevention, assistance, correct behaviour in an emergency.

Method: The British government can look back on many years of experience in terms of awareness-raising strategies. The campaign informs about current threat situations and ways to recognize suspicious behaviour as well as appropriate responses in an emergency. It also offers links and explanations on how to report something anonymously.

Examples of measures in the context of the campaign:
- The film series "If you see something, say something" raises awareness about unusual behaviour in everyday situations.
- The campaign "Run, hide, tell" provides, inter alia, visual aids specifically geared at pupils.

Recommendations

Cornerstones for awareness-raising strategies for the protection of public spaces:

→ **Overriding strategy:** Media and content should be combined in an overall concept. The British ACT campaign is an excellent example.

→ **Broad multi-channel portfolio:** A comprehensive and carefully co-ordinated spectrum of measures that spans many established channels offers the best chance for long-term results.

→ **Bundling competence:** A first step towards a sound overall strategy is to share competences among selected experts.

→ **Combination of communication channels:** A well thought-out combination of different channels should be used to gradually inform the general public about specific events or incidents.

Glossary

> The European SafeCi project contributes in a unique way to increasing safety and security in our cities. The project is held in high esteem by the Luxembourg authorities.
>
> The general understanding of the law and therefore also the perception of police work is based on a higher European ideal.
>
> *Philippe Schrantz, Director-General Police Lëtzebuerg*

Luxembourg

Business Continuity Management (BCM): Tool to identify weaknesses and threats and to develop appropriate countermeasures for the protection of elementary processes or recovery after a disaster and to provide alternative processes.

Big Data: Big Data describes data sets that are particularly large, usually complex, fast-moving and weakly structured and whose interpretation and analysis require special technologies. The term Big Data is also used to describe the technologies used for interpreting the data sets.

CBRN (Chemical, Biological, Radiological, Nuclear): International acronym for the collective term denoting chemical, biological, radiological, and nuclear (hazardous) substances.

EECC: Directive (EU) 2018/1972. European Electronic Communications Code.

Probability: Calculated or estimated likelihood that a certain incident will happen in a geographical reference area in a defined period in the future – which cannot usually be determined precisely (only as an approximation that can be reached by means of qualitative or quantitative methods or a combination of both).

Evacuation: (In case of large events or emergencies) Leading crowds out of a danger zone. (DUDEN Online)

Threat: State or process that, when exposed to it, may result in damage to a subject of protection. (German Federal Office for Civil Protection and Disaster Assistance)

Interdependence: The full or partial mutual dependence of goods or services. (German Federal Office for Civil Protection and Disaster Assistance)

Intervention: Offensive measure to confine danger, in particular to limit the perpetrators' ability to act and attack.

Criticality: Relative measure of the significance of an infrastructure or its components in terms of the consequences that a disruption or malfunction has on the maintenance of the overall service and ultimately on the security of supply of all important goods and services for a society. (German Federal Office for Civil Protection and Disaster Assistance)

Need-to-know Principle: Even if a person has access to secret data/information as a matter of principle, this person should only access information that is actually needed for fulfilling his/her specific task.

Perimeter Protection: Includes all measures to secure real estate (e.g. landscaping, structural or technical measures). The main objectives are to make access for unwanted people and vehicles more difficult and to create a sufficient distance between the public space and the object to be protected.

Resilience: Transformative, cyclical process, that builds capacities in technical, social and organisational resources for critical system function, so as to mitigate the impacts of disruptive events, thus guaranteeing the continued provision of its basic functions.

Risk: In the context of terrorist attacks, risk describes the probability x impact.

RPA/S (Remotely Piloted Aircraft/System): Term used internationally for unmanned aircraft that are controlled remotely by an external controller (pilot).

Impact: Extent of damage that is likely to be incurred at an incident – difficult to quantify (low probability vs. consistently high impact).

Super Recogniser: People with an exceptional ability to recognise and process human faces.

SWOT Analysis: Business term; analysis of strengths, weaknesses, opportunities, and threats.

UAS (Unmanned Aerial System): Term used internationally for unmanned aerial vehicles in conjunction with their control unit.

UAV (Unmanned Aerial Vehicle): Term used internationally for unmanned aerial vehicles (commonly drones) that are operated by remote control or navigate autonomously.

Vulnerability: Measure of a subject of protection's susceptibility to damage with regard to a certain incident.

"

The importance of projects like SafeCi lies primarily in networking and the exchange of experiences. Networks and the exchange of experiences are key instruments for a timely response to current security threats and enable us to learn how to best counter such threats. Projects like SafeCi help us to effectively protect our citizens.

Jan Švejdar, Police President of the Policie České republiky

Czech Republic

Photo Credits

Acknowledgments

Outlook

This publication is an abstract of the manual "European Recommendations for the Protection of Public Spaces against Terrorist Attacks".

The extended version contains a myriad of additional European Best Practices which are described in detail. Moreover, each topic is enlarged upon theoretically and concrete recommended courses of action for the protection of public spaces are presented.

The extended version will be published in May 2021. European police and security authorities can order the extended version from the publisher.

www.berlin.de/safeci