This report was funded by the European Union's Internal Security Fund — Police under grant agreement n° 815356

Public Resillience using Technology to Counter Terrorism

D 5.6 – 2nd PRoTECT Workshop

WP number and title	WP5 – Dissemination and Communication
Lead Beneficiary	Efus
Contributor(s)	DITSS, Eindhoven
Deliverable type	Report
Planned delivery date	31/07/2020
Last Update	15/09/2020
Dissemination level	PU

Disclaimer

The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The PROTECT Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
2	KENTRO MELETON ASFALEIAS	KEMEA	RTO	GR
3	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	RTO	NL
4	INSPECTORATUL GENERAL AL POLITIEI ROMANE	IGPR	GOV	RO
5	FORUM EUROPEEN POUR LA SECURITE URBAINE	EFUS	NPO	F
6	LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS	L3CE	RTO	LT
7	GEMEENTE EINDHOVEN	Eindhoven	GOV	NL
8	AYUNTAMIENTO DE MALAGA	Malaga	GOV	SP
9	DIMOS LARISEON	DL	GOV	GR
10	VILNIAUS MIESTO SAVIVALDYBES ADMINISTRACIJA	VMSA	GOV	LT
11	MUNICIPIUL BRASOV	MUNBV	GOV	RO
12	STICHTING KATHOLIEKE UNIVERSITEIT BRABANT	JADS	RTO	NL
13	MINISTERIO DEL INTERIOR	MIR	GOV	SP

To the knowledge of the authors, no classified information is included in this deliverable

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
EC	European Commission
DG Home	The Commission's Directorate-General for Migration and Home Affairs
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
JRC	Joint research Center
ISPF	Internal Security Fund - Police
DG Move	Directorate General for Mobility and Transport
HR	Hostile Reconnaissance
PTR	PRoTECT Technology Roadmap
PRoTECT	Public Resilience using Technology to Counter Terrorism
TEF	Technology Evaluation Framework
RfI	Request for Information
SLR	Systematic Literature Review
VAT	Vulnerability Assessment Tool
PSOI	Public Space of Interest

Table of Contents

Executive Summary

The PRoTECT project aims to strengthen local authorities' capabilities in public protection by putting in place an overarching concept where tools, technology, training and field demonstrations will lead to situational awareness and improve direct responses to secure public places pre, in, and after a terrorist threat.

The main pillars of the project are **i)** to contribute to the European framework for the protection of public spaces by creating the conditions for better collaboration between municipal authorities and Law Enforcement; **ii)** to fine tune tools for vulnerability and technology assessments by testing the EU vulnerability assessment tool and conducting vulnerability assessment in 5 European Cities and iii) to contribute to the consolidation of a technology roadmap by organising peer to peer exchange with other municipalities with technology solutions and best practices.

An initiative of the Core group of the European Network of Law Enforcement Technology Services (ENLETS), this cross sectoral project is composed of a multi-disciplinary and geographically diverse consortium of 13 partners from 6 different countries (7 governmental institutions of which 5 municipalities, and 2 non-profit organisations and networks).

The project has successfully concluded its first year by **i)** producing a Manual for local authorities to guide them in the use and implementation of the Vulnerability Assessment Tool developed by DG HOME, **ii)** by conducting f vulnerability assessments in the five partner cities, with the help of the EU tool and the manual, **iii)** by publishing a Request for Information and **iv)** by performing a Technology Evaluation with the aid of the Technology Evaluation Framework, to select solutions that can assist in preventing and mitigating terrorist attacks within public spaces.

PRoTECT now enters the demonstration phase in the 5 partner cities of Brasov (RO), Eindhoven (NL), Larisa (GR), Malaga (ES) and Vilnius (LT). The demonstrations will contribute to create insight on possible benefits of exploiting such solutions for the protection of public spaces.

The web seminars were organised within the framework of the dissemination and communication activities of work package 5 in order to invite municipal authorities across Europe to participate in the project and to raise public awareness on the results of the project.

This report describes the PRoTECT Second European Seminar, that took place online, due to the current situation regarding the COVID-19 pandemic. Three sessions of two hours and a half were organised on 15, 16 andv17 July 2020 by Efus and DITSS, and with contribution of consortium partners and with the participation of an audience that consisted of different sectors and countries.

The online seminar had feature exchanges on best practices and technologies that were developed by law enforcement agencies, local authorities, European-funded projects and the private sector. It has given local authorities insights on what criteria to consider when selecting a solution to aid the protection of their public spaces. The web seminar was divided into three sessions, together aiming to provide an overall picture on public spaces at the policy, strategic and practitioners' level:

➔ Session 1 (15 July, 10am CEST) Panel: How to cooperate with a wide range of stakeholders in order to mitigate emerging challenges in protecting public spaces?

This session was hosted by EFUS and DITSS, who invited three panelists representing a complementary vision at the European level on the subjects of cooperation and information sharing, to mitigate challenges related to the securitization of public spaces. The invited speakers are *Andrea Volkmer*, (Policy Officer, DG Home, Counter Terrorism Unit, European Commission) *Sandra Bertin* (Director of Municipal Police, City of Nice) and *Patrick Padding* (Police station and Innovation mission, Core Group leader of ENLETS).

➔ Session 2 (16 July, 10am CEST) Case studies: Existing practices used at the local level for the protection of public spaces

The session was opened by *Giuseppe Cascavilla*, project partner and Postdoc in Data & Service Engineering and Research from the Jeroen Bosch Academy of Data Science (JADS) who gave a key note presentation on the PRoTECT Technology Roadmap, to create understanding and know-how on how to identify and analyse potential (technological) solutions that could aid in protecting public spaces against terrorism.

The keynote speaker's presentation was followed by the presentation on two case studies of locally implemented initiatives to protect public spaces – called *the Servator Project*, which is a national approach within the UK to help society and businesses protect themselves against Hostile Reconnaissance. The *Servator Project* was presented by *Nick Thatcher* from the Metropolitan Police of London. Subsequently, the Berlin Model for *Super-Recognizer identification* (BeMo SR-id) was presented by Dr. Meike Ramon of the University of Freibourg, accompanied by Simon Rjosk of the Berlin Police. The BeMo SR-id is a tech assisted, human-centered assessment of face processing. Super recognizers are human individuals that have the unique ability to recognize more than 80 percent of the faces they have seen. The BeMO SR-id helps police to identify these Super Recognizers within their organisation.

The two case studies represented problems that led to the development of the initiative, the results, the requirements for implementation and their main challenges.

➔ Session 3 (17 July, 10am CEST) How to assess technologies to protect public spaces? The PRoTECT Technology Assessment Framework. Public announcement of the selected solutions for demonstration in the five PRoTECT partner cities-

This session, held by PRoTECT partners *Graeme van Voorthuijsen* (Netherlands Organisation for Applied Scientific Research (TNO)), *Ioannis Chasiotis* (Research Associate, Center for Security Studies (KEMEA)) and *Peter van de Crommert* (Manager EU Projects, Dutch Institute for Technology, Safety & Security (DITSS)), presented the Request for Information (RFI) procedure, that was set up to invite potential tech solutions to be demonstrated in the five PRoTECT partner cities, based on hypothetical threat scenarios in specific public spaces that are potential soft targets for a terrorist attack. PRoTECT's Technology Evaluation Framework (TEF), a unique tool for evaluating such solutions and/or technologies, that local authorities can tailor to their specific needs and vulnerabilities, was also the object of the presentation. Finally, the session concluded with the announcement of the Selected Technological Solutions that resulted from the RFI.

Over 100 participants from Law Enforcement Agencies, municipal representatives, local security practitioners that are responsible for the protection of public spaces, and industrial, national and European stakeholders have participated and have enriched the discussion during the three sessions.

1 Introduction

A year after the first seminar in Brasov (RO), the PRoTECT's project has entered a decisive phase in regards to the selection of solutions that could possibly enhance the protection of public spaces and the demonstrations of such solutions in the 5 partner cities.

The second European Seminar, entitled "Technological and human-centred solutions to protect public spaces against terrorist threats" was planned, to take place in the city of Larisa, Greece. However, due to the crisis generated by the COVID-19 the original event could not be carried out as planned. EFUS and DITSS together decided to adapt the seminar into an online format. The web seminar was divided into three sessions, one session per day, each for one and a half hours.

The objectives of this event were to share the progress made by the project so far with a broader audience and to create conditions to foster discussion and exchange on best practices and technologies developed among a community of relevant stakeholders such as law enforcement agencies, local authorities, European-funded projects and the private sector. One of the seminars objectives was to provide local authorities with insights on what criteria they should consider, when selecting a solution to protect their public spaces.

Over 100 participants from Law Enforcement Agencies, municipal representatives, local security practitioners that are responsible for the protection of public spaces, and industrial, national and European stakeholders have participated and have enriched the discussion during the three sessions.

One of the purposes within PRoTECT was to provide relevant stakeholders, such as the *EU Policy Group on Soft Target Protection from the European Commission* and the *Practitioners and Operators Forum*, with tangible results, such as valuable feedback and practical recommendations that are based on technology and soft target assessment tools. Therefore, an online seminar was organized, aiming to share the building principles of the project regarding cooperation and peer-to-peer exchange. Additionally, the seminar facilitated a platform for European exchange of views on practices and solutions regarding the protection of public spaces from both high-level and practitioner's standpoints.

The deliverable consists of the following chapters:

Chapter 1 – Introduction- a general description of the deliverable's content and layout will be made.

Chapter 2 - Seminar Objectives & Setup – presents the purpose of the seminar, the format of the sessions and the speakers and attendees' profiles.

Chapter 3 – Web Seminar Content – Presents the main points discussed by the speakers and the highlights for consideration for future exchanges and discussions.

Chapter 4 – Web Seminar Evaluation – This chapter presents the results of the seminar evaluation retrieved from customized evaluation form completed by the participants.

Chapter 5 - Conclusions - concludes the report and presents the overall results of the web seminar.

2 Seminar objectives and Setup

2.1 Purpose of the seminar

Local and regional authorities in Europe have taken a number of steps to prevent terrorist attacks and protect their citizens. Developing common guidelines and exchanging good practices are key in order to achieve sustainable and effective solutions. In light of these considerations, local authorities can play a significant role in improving the protection of public spaces, mainly if they are able to identify the vulnerabilities of such spaces and acquire knowledge about existing solutions, both technological and human-centered, that meet their needs.

The online seminar explored such questions by promoting exchanges on best practices and technologies developed by law enforcement agencies, local authorities, European-funded projects and the private sector and also by providing local authorities with insights on what criteria to consider when selecting a solution to protect their public spaces. The web seminar was divided into three sessions:

➔ Session 1 (15 July, 10am CEST) Panel: How to cooperate with a wide range of stakeholders in order to mitigate emerging challenges in protecting public spaces?

A panel composed of three experts representing European Commission's DG HOME, a representative of the local and regional governments in the framework of the Security in Public Spaces Partnership from the Urban Agenda for the EU and a representative of the practitioners from ENLETS, discussed how to cooperate with a wide range of stakeholders in order to mitigate emerging challenges in protecting public spaces.

➔ Session 2 (16 July, 10am CEST) Case studies: The protection of public spaces at practitioners' level

This session focused on the practices used by local authorities. The first part of the session was dedicated to the presentation of an overview of the PRoTECT cities' best practices followed by two case studies that were implemented by municipalities outside the project.

➔ Session 3 (17 July, 10am CEST) How to assess technologies to protect public spaces? The PRoTECT Technology Assessment Framework. Public announcement of the selected solutions for demonstration in the five PRoTECT partner cities.

The third session focused on the presentation of PRoTECT tools that could potentially support local authorities in the evaluation and selection of accurate solutions that respond to the mitigation of public spaces vulnerabilities. In this session the solutions that protect cities have selected to be demonstrated, were announced.

2.2 Participants

In total, 105 people participated in the web seminar, of which 80 were external to the PRoTECT project consortium. Participants came from around 10 countries (Belgium, Germany, Spain, France, Greece, the Netherlands, Romania, Poland, Portugal, United Kingdom and Switzerland). Among the participants were representatives from local authorities and law enforcement agencies, as well as experts, security practitioners and other stakeholders involved at the national and European level.

2.3 Session 1: Session 1 – Panel: How to cooperate with a wide range of stakeholders in order to mitigate emerging challenges in protecting public spaces?

2.3.1 Objective

The main objective of the first session was to promote the exchange between actors involved in security policies and strategies for the protection of public spaces. Thus, the discussion promoted the debate, from a strategic point of view, and information about the obstacles local actors experience, as well as the existing resources at national and European level to solve them.

The session commenced with the statements in the EU Action Plan and the working document on Good Practices to Support the Protection of Public Spaces about the co-production of public spaces protection as a key element, particularly in the context of terrorism. Preventing and mitigating terrorist threats, require raising awareness among local and regional authorities and training them. Furthermore, it is important that they cooperate with each other as well as with the private sector. Increased cooperation is also needed between the local, regional and national levels of governance. What avenues for cooperation exist at the European level regarding the protection of public spaces? How can cities best access funds and training? How can we support peer-to-peer exchange among EU cities? How can we make such coordination and cooperation effective? What are the challenges for the different actors within operationalising a joint action?

2.3.2 Speakers

- ➔ Andrea Volkmer, Policy Officer, DG Home, Counter Terrorism Unit, European Commission
- ➔ Sandra Bertin, Director of Municipal Police, City of Nice– Police station and Innovation mission
- ➔ Patrick Padding, Core Group leader of ENLETS
- ➔ Pilar De La Torre, Projet manager at Efus-Moderator

2.3.3 Session development

In line with the EU Action Plan to Support the Protection of Public Spaces and the staff working document on Good Practices to Support the Protection of Public Spaces, several platforms and working groups have been created to promote the exchange of practices but also to better collaborate and coordinate among security actors.

The Staff working document of the EU mentions the good practices to support the protection of public spaces: **i.)** *Assessment and Planning* (identify potential vulnerability, develop and implement a facility or event security plan and develop and implement a crisis management plan), ii**.)** *Awareness and Training*, **iii.)***Physical Protection* and **iv.)** *Cooperation*.

New venues for cooperation are proposed by the EU in regards to the protection of public spaces that local and regional authorities can access.

Andrea Volkmer mentioned that the Action plan to support protection of public spaces (2017) was conceived to support Member States which are primarily responsible for the protection of public spaces. EU's role as supporter and facilitator looks to set out measures to provide guidance and support to Member States at national, regional and local level in protecting public spaces.

In this respect, the European Commissions established a number of venues for a more systematic and structured exchange of information and sharing of best practices to protect public spaces, as follows:

1. ***EU funding:*** call for project proposals through the Internal Security Fund (ISF) Police. Projects like PRoTECT are funded by ISFP but also other "sister" projects such as Safeci and Stepwise.
2. ***EU Policy Group on Soft Target Protection:*** This group brings together national policy-makers (Member States, police agencies mainly) with the aim of collecting, exchanging and disseminating best practices and advise.
3. ***Operators Forum:*** Brings together public-private representatives, EU associations of different private sectors (malls, hospitality) the staff working document offers a collection of practices.
4. ***Practitioners' Forum***: brings together law enforcement practitioners of the Member States and law enforcement networks.
5. ***Interest groups on Commission's information platform CIRCABC:*** The Communication and Information Resource Centre for Administrations: a collaborative platform, which offers an easy distribution and management of documents. It provides a secured working area to share information with thousands of users and interest groups.
6. ***Technical tools:*** like the EU vulnerability assessment checklist and cooperation with JRC for the organisation of trainings. A digital training program will be available in the autumn of 2020, that focuses on the protection of different kinds of threats. The training will be open to event organisers, but is meant in particular for local stakeholders.
7. ***Networks***: like Efus to disseminate and share information.

The counterterrorism unit of DG Home promotes cooperation with other DGs. For instance, DG Move[1] has been working to produce a tool for helping security managers at larger complex multimodal stations, to identify vulnerabilities against terrorism and other crimes to come up with solutions.

Cities' strategies have evolved within the realm of the protection of public spaces. The Urban Agenda has contributed to this end, by promoting safer public spaces for all and by making local actors aware of their role. Despite this progress, obstacles to innovate and to overcome the technological locks and the legal barriers remain.

Sandra Bertin stressed that the EU's Urban Agenda is an initiative launched in 2016. It is a new, multi-level working method that favours cooperation between Member States, local and regional authorities, the European Commission and other relevant stakeholders in order to improve quality of life and innovation in

[1] DG MOVE produced in 2018 an interactive toolkit to help security managers of large and complex (multimodal) stations to systematically identify risks of terrorism and a range of other crimes in their sites, and use a combination of tested theory, systematically-reviewed evidence and practical experience to come up with plausible interventions appropriate to risk/problem and context. The Toolkit was translated into at least 15 EU languages and can be customised to local regulations etc, and local site conditions.

European cities and to identify and successfully tackle social challenges. One of the objectives is to involve local and regional authorities in the design and implementation of EU policies, while strengthening the urban dimension.
The *Security in Public Spaces Partnership* is a multilevel governance working group, created in 2018, that has contributed to the improvement of local and regional authorities' actions regarding the protection of public spaces. Through this partnership, local authorities, Member States and European institutions will work together to strengthen the role of cities in European security policies, to increase the sharing of knowledge and good practices, and to advocate legislative reform and new funding frameworks at European level.

An Action Plan was developed by the Urban Agenda Partnership on Security in Public Spaces, that identifies three thematic priorities:

1. Urban Planning and Design 'to create safer cities',
2. Technology and Security for Smart and Safe Cities,
3. Managing security and sharing public spaces.

These priorities will be operationalised through a series of actions based on six major points:

1. Develop recommendations in the field of securing public spaces,
2. Develop a framework for self-assessment,
3. AI technologies in urban areas,
4. Integrated urban security training,
5. Social cohesion & security,
6. Guidance on security by design.

The City of Nice is the leader of priority 2. 'Technologies for Smart and Safe Cities' of the Urban Agenda's Security in Public Spaces Partnership. During the sessions, it was mentioned that innovative technologies are multiplying and examples of safe and smart cities are in continuous emergence across the world. Within the context of terrorism, an evolving threat requires an evolving response and an ability to innovate. Including by technological means in order to thwart it. As testers and end-users, cities need incentives and adapted frameworks to use security-related technologies to their fullest potential in compliance with legal requirements and ethical principles.

The main obstacles faced by cities mentioned during the discussion revolved arounds regulations, technical procedures and lack of training:

Sandra Bertin stressed that cooperation with private actors, such as shopping malls, may be blocked by regulations and privacy issues.

Also, related to regulation and private issues local authorities are confronted with too long and technical procedures to implement or test a technology that industrials hardly follow. This creates difficulties when replying to calls for proposals.

Another challenge is the lack of awareness and technical skills of security actors at the local level in terms of technologies and innovation, but also in terms of protective security.

The importance of promoting training and joint exercises to transfer knowledge to the local and regional security actors was mentioned. Patrick Padding from ENLETS illustrated the existing channels to facilitate the exchange of information with local actors and to support the strengthening of their capacities in terms of technologies to prevent and mitigate the effects of terrorist threats.

Patrick Padding explained the practitioners' forum under the EU Policy Group on Soft Target Protection was an initiative of the ENLETS core group to exchange expert knowledge with regards to the protection of public spaces at the Member States level. A High-Risk Security Network has been established, which is supposed to bring together representatives of specialised law enforcement units that are responsible for the protection of high-risk public spaces. In view of training, it was mentioned that this is an extremely important action to take, as technology does not stand in itself. Instead it needs to contain not solely a regulatory framework, but also practice. By providing a platform for common training and joint exercises, the network seeks to support Member States in improving their preparedness against attacks and enhancing their capacity to react in case of an attack.

He stressed that enhanced cooperation between specialised police units and the local authorities is needed. Through trainings, developing joint exercises and share of best practices. This cooperation should be extended to ensure the protection of public spaces of different types (public

, private, semi-public) as well as within the framework of different types of events. Various actions in place are necessary pre, during and after a terrorist attack. For instance, community policing, open source intelligence, vulnerability assessments and transparent communication amongst others. For these different actions, training stakeholders is also necessary.

Local authorities and private operators should be able to conduct security assessments in a continuous way in order to increase awareness and preparedness. In this regard, technology can cut across such actions but needs to be adapted.

Panellists stressed the need to make coordination and cooperation effective among the relevant security actors at all levels: local and regional, national, European, but also to reinforce the cooperation between the public and private sector.

Andrea Volkmer: multi-level cooperation is important and needed. Especially because within the management of public spaces and soft targets, actors of different natures intervene. For example, shopping centres. From the EU level side: projects to develop joint procedures and approaches, and discussion and training regarding threat scenarios that need to be considered. Common exercises are also helpful to test procedures. Local authorities and private operators should come together on a regular basis.

The EU strongly encourages the creation of consortia involving the private sector in its funded projects.

Patrick Padding: *"Urban design for security is crucial for effective cooperation. Joint agreements on information sharing as well. Security and private operators are becoming more and more important to really detect any changes in the city and suspicious behaviour"*.

During the discussion it was frequently mentioned it is challenging for LEAs and other security authorities to associate with private operators. In this respect Patrick Padding also highlighted the challenge of sharing privacy sensitive information.

2.3.4 Main conclusions

- To involve a wide range of stakeholders from a local, national and European level and the private sector, forms a priority within the protection of public spaces. Quite a number of venues for cooperation and existing platforms and tools at the EU level, were shared during the seminars. The most frequently mentioned: **i)** targeted funding made available through European projects within the realm of public spaces protection, **ii)** practitioners and operators fora, **iii)** interest groups that

have been established within the Commission's information platform CIRCABC, meant to establish a library of good practices, **iv)** development of technical tools like the EU vulnerability assessment checklist, and finally, **v)** cooperation with JRC to enhance the training possibilities to local authorities.

- Better coordination between public and private security actors is key for the protection of semipublic spaces. Examples of how this cooperation has been effective were mentioned during the discussion.
- Provide knowledge and training to local authorities to ensure a better protection of public spaces is a priority, to do so it is necessary to foster the exchange of best practices as well as to provide trainings on how local actors can implement a security assessment that allows them to identify potential vulnerabilities, develop and implement a security plan for public spaces and better identify and implement solutions to mitigate the risks.
- Despite the existing mechanisms for cooperation and coordination, it is still challenging for local authorities to keep fluid collaboration and information exchanges among stakeholders. Due to a number of reasons ranging from diverging regulatory frameworks, operational procedures and working cultures this proves to be a challenging aspect.
- In terms of technology adoption, panelists observed that legislative and administrative obstacles are at hand, that make it more complex for local authorities to select and implement technologies for the effective protection of public spaces.

2.4 Session 2 – Case studies: Existing practices used at the local level for the protection of public spaces

2.4.1 Objectives

- Description of best practices and technologies for the protection of urban areas.
- Providing innovative solutions (EU-based) originated from EU research projects in the security domain.
- Providing a technology roadmap for the protection of soft targets in EU cities.

2.4.2 Speakers

Keynote "PRoTECT Best Practices and Technologies on the protection of public spaces"

➔ Giuseppe Cascavilla, Postdoc, Data & Service Engineering and Research, Eindhoven University of Technology (JADS)

Cases studies:

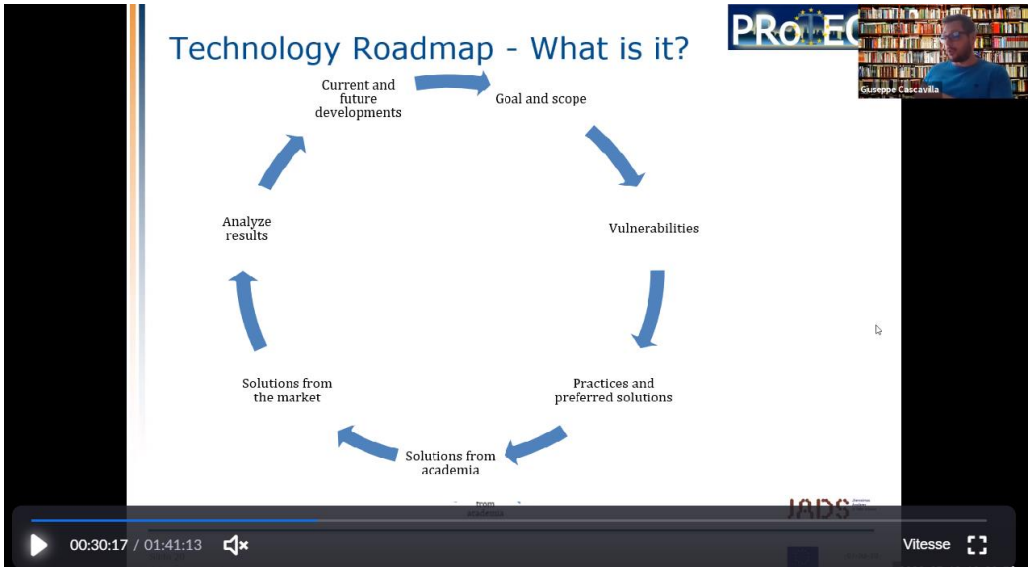
➔ Project Servator, Nick Thatcher, Metropolitan Police of London.
➔ Berlin Model for Super-Recognizer identification (BeMo SR-id), Dr. Meike Ramon, University Fribourg & Simon Rjosk, Berlin Police

Moderator : Tatiana Morales, Project manager et Efus

2.4.3 Session development

2.4.3.1 Keynote: The PRoTECT Technology Roadmap

Giuseppe Cascavilla presented the *PRoTECT Technology Roadmap (PTR)*, a method or tailormade strategic plan to create understanding and know-how to identify and analyse potential (technological) solutions that aid in the protection of public spaces against terrorism. It is meant to be used by local municipalities or LEA's to get an insight into what technologies are and will be in use and to determine what technological solutions to implement regarding their vulnerabilities in countering terrorism. Giuseppe Cascavilla stressed the importance of including experience and preferences by the end users, but also looking at academic and market developments for current and future (technological) solutions.



Giuseppe Cascavilla explained that the Technology Roadmap is divided into 8 phases.

The main findings highlighted by the keynote were:

- There is no one single bullet-proof solution available among the Market, Academia, and Municipality proposed approaches and technologies. Conversely, multiple methods and techniques can be put in place to guarantee safety and security in public spaces.

- The market, followed by the academia, proposed the majority of tools and technologies that are suited for the protection of public spaces. However, most of the time these technologies are not always plug-and-play tools and need a training period in order to be used, rather than a specific type of personnel with appropriate skills for managing information and devices. Moreover, it is important not to forget the price related to this advanced technology. For instance, cameras with night vision and advanced machine learning algorithms have high costs for installation and maintenance.

- Physical barriers and architectural approaches proved to be the most frequently used and available solutions for the protection of public spaces. The price and low cost for maintenance make this approach one of the most efficient ones under the cost-effectiveness analysis. However, overall, it is essential to rethink the combination and the usage of these two approaches. On the one hand, in order to build safer urban places from the design phase on and, on the other hand, to integrate the

physical barriers into the landscape of the city to prevent feelings of fear and insecurity among citizens.

- The gap found within governance and Best Practices should further encourage the market, academia, and municipalities to invest more time and resources in this research field. The knowledge built during these years by the municipalities needs to be further investigated in order to develop specific approaches that are based on the landscape of the city, the position and shape of the PSOI and using the strength and expertise of all the professionals involved in the protection of the municipality.

2.4.4 Cases studies

2.4.4.1 Project Servator (Metropolitan Police of London)

The problem:

- Terrorist attacks require a level of Hostile Reconnaissance (HR) that gives the attacker the information needed to mount a successful attack and the confidence to take action.
- Crowded places and iconic sites usually have multiple business interests with different security provision proportionate to individual risk/threat.
- HR of a high-risk venue can take place from a low risk venue reducing the effectiveness of security provision.
- The public space between sites rarely has dedicated security provision.
- Police are not always there. We needed an approach that would empower the usual site to take steps to frustrate HR.

The solution “The Servator project”:

- The solution will Target Harden the site through empowerment of the usual site users to identify HR and either call police or make an approach.
- The site will become a hostile environment for people with criminal intent. Specially trained officers can then identify these people through their actions.
- This is a national approach that creates an online presence. National Coordination is through City of London Police.
- Police signpost normal site users to other Government Counter Terror training packages designed to prepare the public/businesses for a successful attack.
- Officers work with specialist police units, local government, site management/security, the public and anybody that uses the site as part of ‘normal business’.

The Servator Project aims to deter, detect and disrupt a range of criminal activity, including terrorism, while providing a reassuring presence for the public. Officers are experienced and specially trained to spot the tell-tale signs that someone is planning or preparing to commit an act of crime.

The Metropolitan police of London works with partners, including other police forces, businesses and the public, to continue to protect London and everyone who lives, works or visits here and to make it a difficult place for criminals and terrorists to operate.

Project Servator has been successful in gathering intelligence that has assisted Counter Terrorism Units across the UK in investigating and preventing acts of terror. Results of the work is visible in many arrests for a multitude of offences and is responsible for removing firearms, knives and drugs from London's streets.

Project Servator's patrols are highly visible and can happen at any time and in any location. Officers will talk to the public, local businesses and private security staff to let them know what they're doing and remind them to be vigilant, trust their instincts and report any suspicious or unusual behaviour. Working with the community is a vital part of making Project Servator a success, so if you have any questions, please feel free to talk to our officers.

Servator implementation required:

Police Investment

- ➔ Staff and training
- ➔ Engagement literature
- ➔ Time

Site Investment

- ➔ Time sacrifice to allow training
- ➔ Willingness to be associated with police
- ➔ Willingness to allow police 'footprint' on their on-line presence

In many ways this is an 'idea' to be adopted rather than a product to be bought.

Main Results:

- It must be remembered that this project is one part of a range of complimentary solutions developed by the UK and should not be considered on its own.
- There have been no successful attacks on a site protected by Project Servator, Metropolitan Police. It is probable that this will change.
- Domestic criminals are arrested daily indicating that protected sites are hostile territory for people with evil intent.
- Arrests have been made under Counter Terror legislation.
- There has been an increase in intelligence flow.
- Normal site users report increased satisfaction with police.

Challenges and lessons learned:

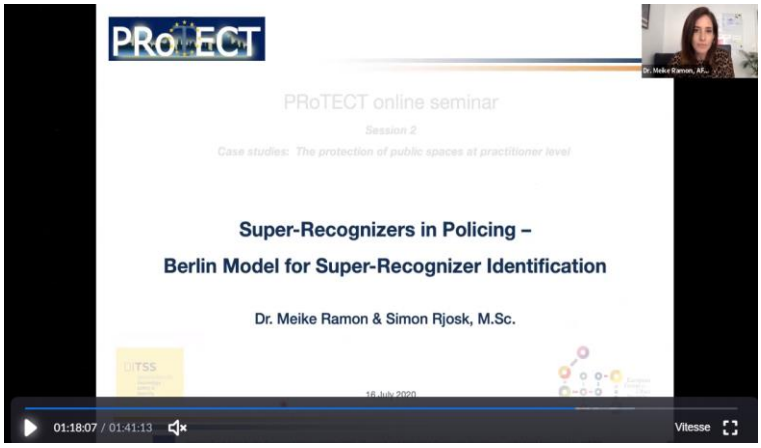
- The biggest challenge is educating the normal site user on Counter Terrorism without increasing alarm or fear.
- This has been achieved by adopting a conversational approach with the public and site staff that is repeated time and time and time again until it becomes routine.

- Small business such as local coffee shops have a good retention rate of staff. Large multi-national businesses have a high turnover of staff. This dilutes the impact of the work.
- This has been addressed by a willingness to repeatedly engage with all level of staff multiple times.
- Internal communications within the police must be good to ensure that all reports of suspicious activity are responded to at protected sites. Trust is hard to build but easy to lose.
- This whole tactic depends upon the police and public communicating with each other.

2.4.4.2 Berlin Model for Super-Recognizer identification in the framework of Safeci project (University of Fribourg and Berlin Police)

The problem:

- The increasing availability of technology, pretty much everyone in the world owns a cell phone or the majority of people does.
- There is a growing demand for image and video processing raising inevitable issues concerning automatic solutions to deal with this increasing volume of image and video processing.
- These issues relate to privacy issues and data protection aspects.



Taking into consideration these two aspects and considering them simultaneously, it makes sense to direct a little more attention towards human solutions that have already been implemented.

Increasing interest in Super Recognizer (SR) deployment in policing was associated with many questions such us what is a super recognizer? Or how should we identify them? Who should be able to identify these super recognizers? And why should we actually implement them? Why should they be deployed? What do we expect by putting them into place? What is the actual outcome that we anticipate and what would justify our desire to continue their implementation?

According to a survey conducted within the project Safeci, people were asked to define what an SR is. The main answers were 1) *someone who never forgets a face*, 2) a *small proportion of the population that can remember 80% of the faces* they've ever encountered, 3) An individual that scored above average in face matching and 4) *people who recognize others based on many different features* such as posture, gait, voice, facial information etc. The survey results highlighted that there is no consensus on a single definition of an SR, nor on how the SRs should be identified.

For police practitioners generally super recognizers are people who can recognize people so that they can use a multitude of different types of sources of information to recognize someone, whereas the definitions among the public were quite mixed. There are very different definitions among practitioners and researchers who focus on face processing, when they think about super recognizers and civilians who have a mixed definition.

In regards to the question of how to identify an SR, the problem is that the existing methods are not optimal to identify super recognizers. What's needed is actually a solution for Super Recognizer identification that's

developed specifically to meet the demands of the police agency in question or police practitioners in general.

The solution:

- The proposed solution is the Berlin model for Super Recognizer identification. It combines expertise procedures from a scientific research background, as well as practices that are common to policing. It is a technology assistant but human centred assessment tool. It rests on utilizing technology to identify individual differences in human ability and processing faces using police relevant psychometric testing, so tools that could be used in the lab but transferred into a police relevant context.
- The process revealed that predominantly tasks of police interest involved image search and comparison, as well as some type of search and survey into a surveillance activity. And image search and comparison could involve any type of analysis of image or video material in, for instance, for the goal of grouping crime series or preventing crimes, but also, for instance, analyzing images where biometric solutions actually failed, because there are certain types of masking that people can apply, which make it impossible for automatic solutions to actually process these faces as being a face in the first instance. And of course, humans are not fooled by these types of things.

Main Results

- With this tool, police have a state-of-the-art assessment of face processing tool which combines both science and policing aspects. Critically, it is relevant for police because it uses case study material. Additionally, this material has been embedded into professionally relevant tasks. The SR Identification Model is a scientific tool, which ensures the internal and external validation of the results, meaning the predictive ability of the model has been statistically validated and the results can be generalized to large populations.

Challenges:

- Clarity, both in terms of definitions and expectations, lack of transparency when it came to previously implemented procedures in the context of policing and research. The challenges faced were inevitably related to the very strict data protection laws in Berlin.
- A lesson learned was the interdisciplinary work, which creates these bilateral learning opportunities that will create a solution that will be more sustainable, and more promising in terms of outcome.
- The Berlin model will almost certainly provide a way to evaluate the deployment of Super Recognizers across different operational settings and tasks.

2.4.5 Main conclusions

- There is no one single bullet-proof solution available among Market, Academic, and Municipality approaches and technologies.
- The gap found in Governance and Best Practices should further encourage the Market, Academia, and Municipalities to invest more time and resources in this research field.
- It must be remembered that technological solutions are part of a range of complementary solutions used for protecting public spaces and they should not be considered on their own.
- It is important to pay more attention to Human-Centred solutions, such as investing in trained staff who are able to associate with communities and private sector participants such as small businesses, who are the first valuable key players in the identification of suspicious activities and persons.

- Working with the community is a vital part in the protection of public spaces by reporting anything deviant, for example, an unattended item or someone acting suspiciously.
- Adopting a tailor-made solution brings objectivity, relevance and learning opportunities to the needs of end users, but also requires solid efforts, collaboration and capacity to comply with strict data protection laws.
- When selecting a solution, it is important to ensure that it does not have the opposite effect on citizens' feelings of insecurity.

2.5 Session 3 - How to assess technologies to protect public spaces? The PRoTECT Technology Assessment Framework. Public announcement of the selected solutions for demonstration in the five PRoTECT partner cities.

2.5.1 Objective:

The main objectives of this session were:

- To present the Request for Information (RFI) procedure to present potential solutions to be demonstrated in the five PRoTECT partner cities. This procedure devises hypothetical threat scenarios in specific public spaces that are potential soft targets for a terrorist attack and can greatly help municipalities to assess existing solutions to prevent or mitigate such attacks.
- To present the PRoTECT's Technology Evaluation Framework (TEF), a unique tool for evaluating such solutions and/or technologies, that local authorities can tailor to their specific needs and vulnerabilities.
- To announce the Selected Technological Solutions coming out of a RFI.

2.5.2 Speakers

➔ Graeme van Voorthuijsen, Netherlands Organisation for Applied Scientific Research (TNO)
➔ Ioannis Chasiotis, Research Associate, Center for Security Studies (KEMEA)
➔ Peter van de Crommert, Manager EU Projects, Dutch Institute for Technology, Safety & Security (DITSS)

2.5.3 Content

2.5.3.1 PRoTECT Technology Evaluation Framework (TEF) and its application

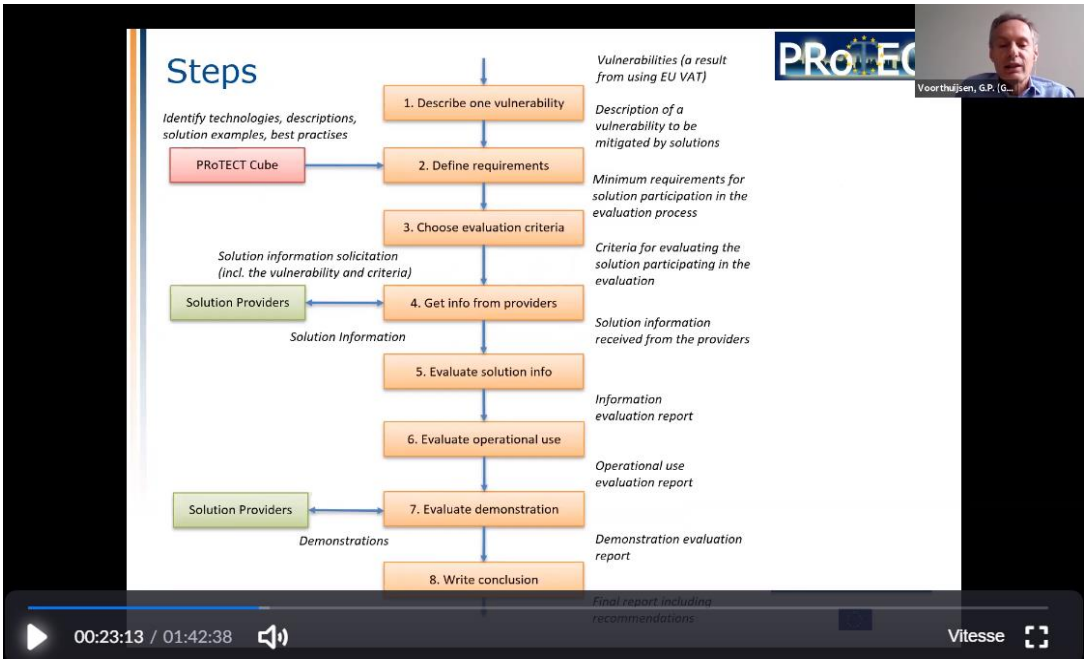
As explained by Graeme van Voorthuijsen, the Technology Evaluation Framework aims to evaluate potential solutions that can help identify vulnerabilities within the general public and public spaces of interest (PSOI) that have been identified by either a council or municipality as an area that could potentially be vulnerable against terrorist attacks.

The TEF was developed to be used by municipalities and usually in conjunction with various stakeholders within the municipality.

The framework can be applied to find relevant technology solutions, and to evaluate technologies within the context of one particular vulnerability. An important part of using the framework is identifying the

participants. These could be individuals from within the municipality, but also external experts and stakeholders.

The tool consists of eight steps of which many are optional. They can be applied to various degrees and not all of the team of expert members will actually be carrying out all the steps in the framework. After setting up a group of experts that were going to set up the RfI, demonstrations and evaluate the technologies, the **1)** first step is to confirm what vulnerability is to be addressed by each city. In the framework of the PRoTECT project, an EU vulnerability assessment Manual was developed, that could be used for the aforementioned vulnerability assessment process. The **2)** second step is to form requirements - if possible - and a discussion with relevant experts. The **3)** third step is to decide on the evaluation criteria for the requested technologies. The **4)** fourth step is to perform the RfI, which conducted soliciting the market for potential (technology) solutions. The **5)** fifth step is to perform an evaluation of the technology responses in a workshop with all relevant experts. The evaluation is based on a specific evaluation method, being a *multi-criteria analysis* that has been tuned to the goal of PRoTECT. The **6)** sixth step is an optional step to also perform an operational use evaluation, using relevant scenarios. The **7)** seventh step is to perform a demonstration of one or more potential viable technologies for the specifically addressed vulnerability in each city. The **8)** eight step is to analyze the results of all evaluations and to write a report for future usage of the tool.



The team should determine for each of the one, two or three evaluation reports, to what degree the goals were met, the consequences of any shortcomings found in the products, and to identify any lessons learned from executing the framework, etc.

The team should also discuss the results from all the reports and form an opinion on the product's suitability in order to mitigate the vulnerability and draw conclusions. Recommendations should also be discussed on further implementation of the product, including more research if necessary.

Write final report

The findings from the product information evaluation, the operational use evaluation and the demonstration evaluation should be summarised in a final report, including the conclusions and recommendations.

Result

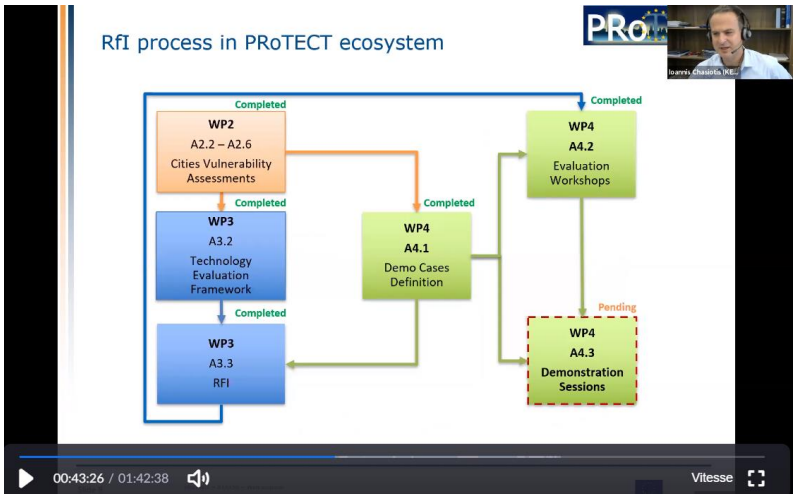
This step should be wrapped up with a report containing the following information:

- The vulnerability details from Step 1 (as context)
- Documentation of, or references to, all steps taken in the framework
- The considerations in the analysis of the evaluation reports
- To what degree the goals have been met, which were set in Step 2
- The conclusion including recommendations

TEF leads to a final report which discusses the results of all evaluation reports, the final conclusion regarding the degree to which the objectives concerning the mitigation of the vulnerability have been met (set in Step 2) and any recommendations concerning the acquisition or future use of the solution for the municipality.

2.5.3.2 Request for information (Rfi)

Ioannis Chasiotis provided a general overview on the Request for Information process run in the context of PRoTECT, for evaluating solutions that are available on the market and/or from research projects, available for facilitating local governments into addressing any vulnerabilities that they might have.



The Rfi aims to constitute a flexible method for collecting information regarding specific issues. However, this method can be adapted - and has been adapted - to the purpose of our project, to scan for solutions for a specific security problem based on the vulnerability assessments. In this regard, local governments may be able to exploit the Rfi methodological approach towards identifying ideas for addressing threats, mitigating risks, and in generally enhancing the sense of security.

Furthermore, this tool could be used for evaluating and prioritizing the identified solutions and aiming in the end to proceed to the validation. Identifying and increasing the cost efficiency and cost effectiveness of the security measures either being currently applied and or how these are going to be affected through the potential exploitation of solutions. Moreover, provide an early indication on improving the law enforcement agencies capabilities to address attacks.

The Rfi has built a series of hypothetical case scenarios that describe what solutions were required. The aim was to locate high tech solutions and ideas that could address the demonstration needs.

Once collected, an important number of solutions provided by tech companies that have responded to the Rfi, the municipalities proceeded to evaluate the solutions while using the aforementioned TEF. It was the perfect occasion to test the TEF criteria and categories. Individual evaluation workshops were held in each of the five PRoTECT cities, with the support of local stakeholders (either remotely or in person).

2.5.3.3 *Announcement of the Selected Technological Solution coming out of a RFI.*

Peter van de Crommert, the PRoTECT project coordinator, announced the selected technological solutions coming out from the Request for Information process within the framework of the project.

The PRoTECT Request for Information (RfI) addressed available solutions that were oriented on protecting/combating terrorism and its effects regarding to open public spaces. The aim of the process, based on hypothetical scenarios dictated by the municipalities of Brasov (RO), Eindhoven (NL), Larisa (GR), Malaga (ES) and Vilnius (LT) (members of the PRoTECT project consortium), has been to investigate the benefits of potentially exploiting available solutions towards preventing and mitigating terrorist attacks within public spaces (so called "soft targets").

The submission procedure remained online for a period of 2 months (1st of April until 1st of June 2020) and in total 35 submissions of solutions have been received. Given that each solution could be applied for multiple municipalities, finally, the submissions for each city were:

- 21 to the municipality of Larissa
- 26 to the municipality of Eindhoven
- 24 to the municipality of Malaga
- 26 to the municipality of Vilnius
- 22 to the municipality of Brasov

Following independent assessments by each of the five partner municipalities cities (via local evaluation committees) and aggregation / confirmation of the corresponding results by the project's General Assembly, 25 Solutions (in total) were selected to be invited to demonstrate their solution in one of the 5 cities. The selected solutions can be found on the PRoTECT Web Site.

The selected solutions will be invited to provide a demonstration (proof of concept) on selected sites by the relevant partner municipalities. Municipalities hosting the demonstrations will compensate the solution providers for the eligible costs up to a maximum as mentioned in the Rfi document and within the limits of the relevant budget available to each of the hosting cities.

2.5.4 Main conclusions

- Local authorities, within their role of safeguarding public spaces and citizens and protecting them against terrorist threats and mitigating vulnerabilities, need to associate technological solutions to human centred approaches, but often don't possess the required tools or knowledge to adequately identify, evaluate and select the potential technological solutions available in the market.
- The Technology Evaluation Framework (TEF) is part of the tools developed in the framework of PRoTECT, with the aim of facilitating local authorities' actions to improve public space security. The eight aforementioned TEF steps, lead to solution information, operational use and evaluations of demonstrations that allow local actors to assess the degree to which the objectives concerning the mitigation of a vulnerability have been met and devise recommendations concerning the acquisition or future use of the solution for the municipality.
- The Request for Information (Rfi) is a method for collecting information about specific issues for facilitating decision making and scanning of solutions to a given security problem. The selection of solutions from a list of prioritized solutions can lead to a demonstration of such solutions. In the case of PRoTECT the process has allowed the consortium to identify an important number of solutions from AI technologies, sensors, physical barriers, drones etc. This process will allow decision makers in municipalities to acquire knowledge on existing solutions and validate their applicability in the context of specific demo scenarios.

- The tools developed in PRoTECT can aid municipalities in gaining situational awareness and improve direct responses to secure public places pre, in, and after a terrorist threat. The ultimate benefits of such tools can result in increasing cost-effectiveness of security measures, gaining operational insights and assessing whether there are any solutions at all for a given vulnerability.

3 Web Seminar evaluation

- More than 100 participants from Law Enforcement Agencies, municipal representatives, local security practitioners responsible for the protection of public spaces, and industrial, national and European stakeholders have participated and enriched the discussions during the three sessions.

- An evaluation survey was launched right after the last session of the seminar. The results of the survey showed that the participants found the seminar very satisfactory (4.7 over 5).

- Regarding the content of the seminar, the participants expressed that in general everything was good, they suggested to ask participants to give 1 or 2 questions beforehand. The case study session was highly appreciated and they suggested to present more experiences used by LEAs in the same format.

> "I actually liked that this was done over the web - I am unable to travel at the moment so I was happy to be able to participate"

- Concerning the web seminar format, participants appreciated the fact that this seminar was online and open to the public. The results of the survey showed that the participants found the seminar format very satisfactory (4.8 over 5). Combining a high level (strategical and policy panel) the first day, with a more practical session with case studies on the second day and presenting the tools resulting from the project the third day, was very much appreciated.

> "I really liked the range of speakers. It was helpful to me as a supplier to hear from the potential users of my company's products and services"

- In terms of the format, participants suggested to dedicate more time to the Q&A and exchange with the audience.

4 Conclusions

The purpose of this document is to present all information given by the speakers and the participants of the second European Seminar, in order to give a general outcome of its results. Taking into consideration the exceptional circumstances dictated by the COVID-19 pandemic, answers that resulted out of the questionnaire proved that the seminar was successful both in terms of *format* (online and spread over three consecutive days, with a balanced duration of 1.5 hours per session) and in terms of *content* (good balance between the more high-level policy discussions on the first day and the more practical sides constituted by the case studies and the presentation of the PRoTECT tools of the second and third day).

Overall, the discussions over the three days shed light onto the different challenges and opportunities for local authorities and security actors regarding the protection of public spaces. Despite efforts to achieve successful coordination with a wide range of stakeholders, facilitated by a number of existing venues for cooperation at the EU level, the sessions highlighted the fact that better coordination between public and private security actors is key to overcome the existing challenges for local authorities to keep fluid collaboration and information exchange among stakeholders. Fluid collaboration and information exchange is of high importance due to a number of reasons, ranging from diverging regulatory frameworks, operational procedures and working cultures.

It was also highlighted that training local authorities to help them build better protection of their public spaces against terrorist attacks is a priority, to enable that process, it is necessary to foster the exchange of best practices and arrange a regularly joint table top or organize real exercises in order to detect shortcomings and to tackle issues related to timely and proper response and task division. Exercises should involve all relevant stakeholders to maximize the outcome.

In terms of technology adoptions and solutions, challenges remain, due to diverging regulations and restrictive legal schemes but also since there is not a one-size-fits-all solution and technology available. Tools should be viewed as being complementary to each other, together forming a strategic solution.

Finally, ethical, and societal considerations are a vital part of the equation when it comes to evaluating the adoption of solutions and the impact on the feeling of (in)security of citizens. A more human centred approach is to be associated to technological solutions by local authorities, within their role of ensuring public spaces and citizens protection against terrorist threats and mitigate vulnerabilities but oftentimes they do not possess the required tools or knowledge. Adaptable tools such as the ones offered by the PRoTECT project and further trainings are very much welcomed.

Concluding, participants left the web seminar with a high satisfactory level, a feeling of great understanding of the public spaces' protection topic and with a great level of interest to increase their knowledge on the subject and to pursue the debate at the EU multi-stakeholder level.

For the project consortium partners, this web seminar was an important milestone in the consolidation of the project activities and the preparation of the remaining ones. The web seminar marked by the announcement of the solutions selected from the Rfi process that will be the object of demonstrations in the partner cities, will contribute to the improvement of the technology roadmap and therefore create a sustainable and long-term contribution to the European framework for the protection of public spaces.

References

[1] PRoTECT Deliverable D2.1 "Manual for vulnerability assessment"

[2] PRoTECT Deliverable D2.1 Vulnerability Assessment Tool

[3] PRoTECT Deliverable D3.1 State of the Art (preferred solutions of the cities)

[4] PRoTECT Deliverable D3.2 Technology Evaluation Framework

[5] PRoTECT Deliverable D3.4 Technology roadmap (overview of the solutions)

[6] PRoTECT Deliverable D4.2 Request for Information

ANNEX II AGENDA IN PROTECT WEB SITE

SAVE-THE-DATE

PRoTECT online seminar

"Technological and human-centred solutions to protect public spaces against terrorist threats"

15, 16 and 17 July 2020

The PRoTECT Consortium is organising the 2nd European PRoTECT seminar on the protection of public spaces on 15-17 July. It will include three online sessions of a duration of 1h30 each.

Event: European online seminar

Description:

Local and regional authorities in Europe have taken a number of steps to prevent terrorist attacks and protect their citizens. Developing common guidelines and exchanging good practices are key in order to achieve sustainable and effective solutions. In correlation to these considerations, local authorities can play a significant role in improving the protection of public spaces, mainly if they are able to identify the vulnerabilities of such spaces and acquire knowledge about existing solutions, both technological and human-centred, that meet their needs.

The online seminar will feature exchanges on best practices and technologies developed by law enforcement agencies, local authorities, European-funded projects and the private sector. It will give local authorities insights on what criteria to consider when selecting a solution to protect their public spaces. The project's five partner cities will share their experience in using the PRoTECT tool and in selecting a solution for demonstration.

Law enforcement agencies, municipal representatives, local security practitioners responsible for the protection of public spaces, and industrial, national and European stakeholders are invited to take part in this event. You can attend either all three or any sessions of your choice. Registration is compulsory for each session and free of charge.

→ Session 1 (15 July, 10am CEST) Panel: The protection of public spaces at policy and strategy level

Register

→ Session 1 (15 July, 10am CEST) Panel: The protection of public spaces at policy and strategy level

Register

The EU Action Plan and the working document on Good Practices to Support the Protection of Public Spaces state that the co-production of public space protection is key, particularly in the context of terrorism. Preventing and mitigating terrorist threats require raising awareness among local and regional authorities and training them. Furthermore, it is important they cooperate with each other as well as with the private sector. Increased cooperation is also needed between the local, regional and national levels of governance. What avenues for cooperation exist at the European level regarding the protection of public spaces? How can cities best access funds and training? How can we support peer to peer exchanges among EU cities? How to make such coordination and cooperation effective? What are the challenges for the different actors in operationalising a joint action?

→ Session 2 (16 July, 10am CEST) Case studies: The protection of public spaces at practitioner level

Register

"There is no one single solution available, conversely, multiple methods and techniques can be put in place to guarantee safety and security in public spaces. The techniques range from architectural design in order to rethink the design of public spaces keeping security into account in continuity to emerging technologies such as AI and predictive surveillance. Moreover, whenever new technologies could appear to be expensive in cost and questionable regarding privacy, or when it could be difficult to rethink and re-project public spaces, building an action plan in order to mitigate, prevent and manage crime events would be a viable solution" (PRoTECT Best Practices and Technologies).

This session will present an overview of the PRoTECT best practices and case studies implemented by cities for the protection of public spaces.

→ Session 3 (17 July, 10am CEST): The PRoTECT project's perspective on the protection of public spaces

Register

Devising hypothetical threat scenarios in specific public spaces that are potential soft targets for a terrorist attack can greatly help municipalities assess existing solutions to prevent or mitigate such attacks. The European Union's Technology Evaluation Framework (TEF) is a unique tool for evaluating such solutions and/or technologies, which local authorities can tailor to their specific needs and vulnerabilities. This session will present the Request for Information procedure to identify potential solutions to be demonstrated in the five PRoTECT partner cities, the use and application of the TEF, and the

End of document