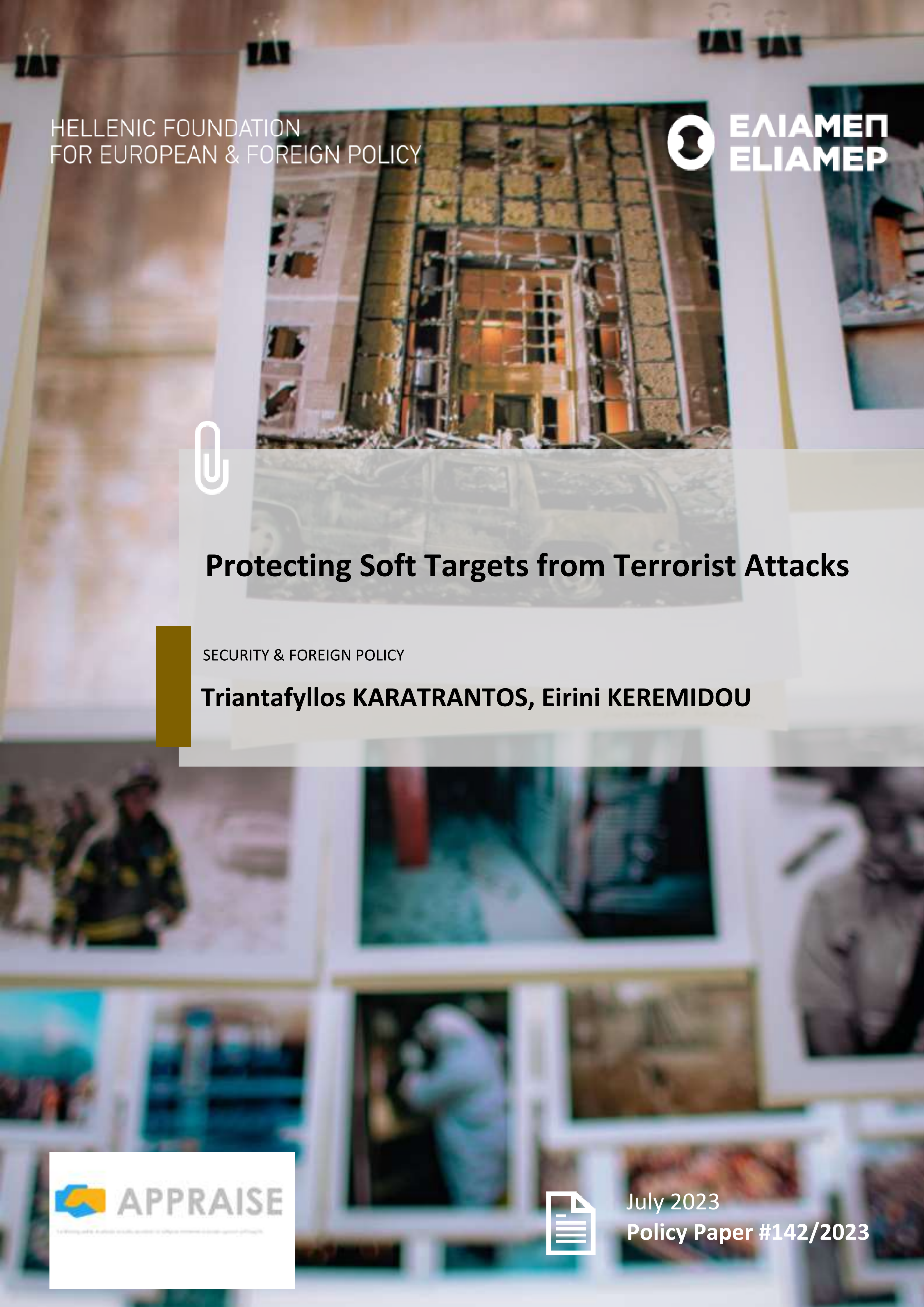

HELLENIC FOUNDATION
FOR EUROPEAN & FOREIGN POLICY

ΕΛΙΑΜΕΠ
ELIAMEP

Protecting Soft Targets from Terrorist Attacks

SECURITY & FOREIGN POLICY

Triantafyllos KARATRANTOS, Eirini KEREMIDOU

APPRAISE

July 2023
Policy Paper #142/2023

ELIAMEP | Policy Paper #142/2023

Protecting Soft Targets from Terrorist Attacks

HELLENIC FOUNDATION FOR EUROPEAN & FOREIGN POLICY (ELIAMEP)
49, Vasilissis Sofias Ave., 10676, Athens, Greece
Tel.: +30 210 7257 110 | Fax: +30 210 7257 114 | www.eliamep.gr | eliamep@eliamep.gr

ELIAMEP encourages open, pluralistic dialogue based on arguments and facts. The views expressed by associates of ELIAMEP are entirely their own and are not binding on the Institution.

Triantafyllos KARATRANTOS
Senior Research Fellow, ELIAMEP

Eirini KEREMIDOU
Research Fellow, APPRAISE project, ELIAMEP

The APPRAISE project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101021981

Summary

- Terrorist attacks, and mainly those launched in 2015-2018, have shown a recurrent targeting of public spaces as part of the perpetrators' modus operandi.
- Considerable attention has been paid in many countries to methods and techniques which can enhance the security of soft targets and provide protection for public places.
- While Member States are primarily responsible for the protection of soft targets, the EU still plays an important role.
- Some attacks were complex and high-intensity (combining explosives and firearms), others were "low tech" and carried out with everyday items such as a vehicle for ramming or a knife for stabbing.
- The European Commission defines soft targets as locations that "are vulnerable and difficult to protect and are also characterised by the high likelihood of mass casualties in the event of an attack".
- The "Security by Design" approach introduces the concept and practical implementation of building security into the design and redesign of public spaces.
- The protection afforded to Europe's citizens can benefit from the effective cooperation between both public authorities and private security practitioners.

Introduction

Terrorist attacks, and mainly those launched in 2015-2018, have shown a recurrent targeting of public spaces as part of the perpetrators' modus operandi, which seeks to exploit the intrinsic vulnerabilities stemming from the open and public nature of "soft targets". Soft targets include pedestrian precincts, tourist sites, transport hubs, shopping malls, places of worship, outdoor markets, concert halls and city squares, and have been targeted in Barcelona, Berlin, Brussels, London, Manchester, Nice, Stockholm et al.

Terrorist attacks, and mainly those launched in 2015-2018, have shown a recurrent targeting of public spaces as part of the perpetrators' modus operandi.

In response to this threat, considerable attention has been paid in many countries to methods and techniques which can enhance the security of soft targets and provide for places that would otherwise remain entirely unprotected. This has resulted in the issuing of a considerable number of guidance and best practice documents; however, since have not taken the form of official standards, they may be off the radar for some all security officers, premise owners, building designers and other relevant professionals.

While Member States are primarily responsible for the protection of soft targets, the EU still plays an important role and has had a holistic policy framework in place since its 2017 Action Plan. Research projects and new technologies are important facets of both EU policy and actions for the protection of soft targets which take into consideration the need for balance between security and privacy interventions. Within this framework, the APPRAISE project is elaborating a new approach to protecting soft targets from terrorist attacks. The aim of this policy brief is to appraise stakeholders and policy makers of the specific challenges posed by soft-target protection, as well as of the EU policy framework and specific best practices and guidelines. The brief ends with a set of policy proposals based on the work of APPRAISE.

Research projects and new technologies are important facets of both EU policy and actions for the protection of soft targets which take into consideration the need for balance between security and privacy interventions.

Why Soft Targets?

The terrorist attacks of the period 2015-2020 have shown a recurrent targeting of "soft targets". Typical examples are the attacks in Barcelona, Berlin, Brussels, London, Manchester, Nice and Stockholm. Some of these attacks were complex and high intensity (combining explosives and firearms), while other were "low tech" and carried out with everyday items such as a vehicle for ramming or a knife for stabbing. Threat assessments by Europol and the EU Intelligence and Situation Centre (INTCEN) confirm this focus in target selection.

Unfortunately, as a trend, attacks against soft targets began prior to the last seven years. According to Tomas Zeman, who coding of selected soft targets based on the GTD Codebook, with the number of incidents and the mean number of casualties, there were at least 275 attacks against soft targets between 2000 and 2015[1]. The majority of the attacks, as the following table shows, were launched against place of worship, trains, places of entertainment/culture/sport, restaurants and cafes, and public areas.

[1] T. Zeman, (2020), "Soft Targets: Definition and Identification", *AARMS*, Vol. 19, No. 1, pp. 109-119.

Target	Number of Incidents
places of worship	63
Trains	44
Entertainment / cultural places / stadiums	36
restaurants / café- bars	29
Public areas	23
Hotels / resorts	19
Schools / educational facilities / universities	15

Table 1: Attacks against soft targets in Europe, 2000- 2015.

Furthermore, the report published by the Tony Blair Institute for Global Change estimates that an average of 17 civilians per day were killed by terrorist attacks, often as a direct result of coordinated campaigns against civilians and public spaces[2].

...we have also many attacks against soft targets from politically motivated perpetrators, especially on the Far Right, as the attacks launched by Anders Breivik in Norway and the attack in Hanau, Germany, show.

Year	Country	Target	Victims	Perpetrator
2004	Spain	Train system of Madrid	193 deaths 2005 injuries	Al Qaeda
2005	United Kingdom	London transport system	56 deaths 784 injuries	Al Qaeda
2011	Norway	Public building & summer camp	77 deaths 319 injuries	Anders Breivik
2015	France	Stade de France, cafes & restaurants, Bataclan theatre	137 deaths 413 injuries	ISIS
2016	Belgium	Zavetnem airport, Maalbeek metro station	35 deaths 340 injuries	ISIS
2016	France	Promenade Des Anglais, Nice	87 deaths 434 injuries	ISIS
2017	Spain	La Rambla Street	24 deaths 152 injuries	ISIS

Table 2: The worst terrorist attacks against soft targets in Europe

The attacks of the last years—and the deadliest of them, in particular, in Paris, Manchester, Barcelona and Brussel—indicate that attacks against soft targets and individuals are mainly part of the modus operandi of jihadist terrorist groups. However we have also many attacks against soft targets from politically motivated perpetrators, especially on the Far Right, as the attacks launched by Anders Breivik in Norway and the attack in Hanau, Germany, show. We should also note that these attacks were

[2] Tony Blair Institute for Global Change, (2018), How Islamist Extremists Target Civilians, Paper, https://www.institute.global/insights/geopolitics-and-security/how-islamist-extremists-target-civilians

perpetrated by both groups and lone actors. It is thus clear that the threat against soft targets is both complex and diverse.

… the European Commission defines soft targets as locations that "are vulnerable and difficult to protect and are also characterised by the high likelihood of mass casualties in the event of an attack".

Definition of soft targets and challenges posed by their protection

Although soft targets are not defined in any international legal framework, a consensus has been reached in recent years on their identification. In its *Fourth progress report towards an effective and genuine Security Union*, the European Commission defines soft targets as locations that "are vulnerable and difficult to protect and are also errorismzed by the high likelihood of mass casualties in the event of an attack"[3]. Furthermore, the EU Action Plan to Support the Protection of Public Spaces provides a general framework within which soft targets as described as vulnerable sites that are easily accessible and open to the public, thereby imposing limitations on security planning and measures. The main categories of soft target are transportation systems (e.g. airport terminals, railway & bus stations, subway systems, ferries), places of religious worship (e.g. churches, mosques, synagogues, temples), weddings, funerals, schools, hospitals, dormitories, market places, indoor shopping malls, museums, tourist destinations, hotels, restaurants, night clubs, theatres, cinemas, landmarks and iconic buildings of symbolic value, venues for special events, (e.g. sport stadiums, cultural arenas, concert halls), long queues of people at the entrance to event sites, and pedestrian zones in urban areas. We should note that the meaning of the term changes depending on the context and type of discussion (policy, legal, operational, technical).

…the primary responsibility is still at the member-state level, and that is a key challenge in the search for a common, coordinated and effective response at the European level.

Despite the EU framework for the protection of Public Spaces and Soft Targets, the primary responsibility is still at the member-state level, and that is a key challenge in the search for a common, coordinated and effective response at the European level. Over and above this very important challenge, we can identify different vulnerabilities that expose soft targets to terrorist threats. These include a reluctance to enhance security due to an underestimation of the likelihood and/or impact of a terrorist attack. Another potentially relevant factor is "security fatigue": outside periods of heightened vigilance, which usually occur in the aftermath of a terrorist attack, sustaining a culture of security may be a difficult long-term attitude for site operators, the public and other stakeholders to develop. Other cultural factors to be taken into account include the extreme sensitivity of places of worship, plus in some cases the suspicion with which a given religious community may view the police and intelligence agencies.

…extreme sensitivity of places of worship, plus in some cases the suspicion with which a given religious community may view the police and intelligence agencies.

Another important parameter are legal/regulatory and institutional obstacles to intelligence sharing and multiagency cooperation. Insufficient inter-agency coordination due inter alia to regulatory gaps and unclear divisions of labor can create crucial vulnerabilities. In addition, intelligence agencies may encounter legal obstacles to their disclosing classified information to operators of vulnerable sites. The financial factor is also important. Many soft targets and public spaces have limited budgets available for security, while security measures can be costly to implement when they require physical changes, additions to infrastructure, the contracting of new security companies, or the hiring and training of personnel. In addition, they may not be able to rely on financial incentives (e.g., funding, subsidies, tax breaks) to support the implementation of security upgrades.

[3] COM/2017/041 final. Fourth progress report towards an effective and genuine Security Union. Luxembourg, Publications Office of the EU, 2017.

To sum up, the main challenges and vulnerabilities are the following:

- the variety of public places that have been or could be targeted;
- the different characteristics of soft targets, which range from fully open spaces to areas with some form of protection;
- the variety of actors involved in the protection of such sites;
- the risk of mass casualties;
- the imperative to strike a balance between improving security and preserving the open nature of public spaces, ensuring that citizens can continue about their daily lives.

…security measures can be costly to implement when they require physical changes, additions to infrastructure, the contracting of new security companies, or the hiring and training of personnel.

European Union Policy Framework

"*We need to safeguard the open nature of these spaces while at the same time making them more secure through stronger physical protection measures that do not create fortresses and still allow people to walk about freely and safely.*"[4], (Counter Terrorism Agenda, 2020).

Although the Member States are primarily responsible for the protection of soft targets, the EU has developed an important policy framework for the protection of soft targets. The main pillars of EU policy are: a) balanced interventions, as technical solutions need to be sought that can help to make public spaces more secure, while at the same time preserving their open and public nature; and b) the "security by design" concept, which need to be integrated into their development from an early stage.

Security by design is built upon the principles of proportionality, multi-functionality, sustainability, accessibility and aesthetics. It stands diametrically opposed to the creation of urban fortresses.

The "Security by Design" approach introduces the concept and practical implementation of building security into the design and redesign of public spaces. It does so while providing information on terrorism risk assessment, project planning, and management. It proposes innovative technical solutions for the protection of public spaces against terrorist attacks. Security by design is built upon the principles of proportionality, multi-functionality, sustainability, accessibility and aesthetics. It stands diametrically opposed to the creation of urban fortresses.

The support the EU can provide for the protection of soft targets is twofold. First, it can foster the exchange of best practices across borders through targeted funding as well as networks of practitioners and guidance material. Second, the EU can involve a wide range of stakeholders from both the local level and the private sector (i.e. the EU Forum on Protection of Public Spaces)[5].

[4] European Commission, (2020), A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final
[5] https://ec.europa.eu/futurium/en/security-public-spaces/eu-forum-protection-public-spaces.html

Action Plan to Support the Protection of Public Spaces (2017)

Good Practices to Support the Protection of Public Spaces (2019)

EU Security Union Strategy (2020)

Counter- Terrorism Agenda (2020)

Fig. 1: The EU Policy framework for the Protection of Soft Targets

While there can never be 'zero risk', these operational measures will help Member States detect threats, reduce the vulnerability of public spaces, mitigate the consequences of a terrorist attack, and improve cooperation.

The first important policy document at the EU level was the Action Plan to Support the Protection of Public Spaces in 2017. The Action Plan sets out measures designed to provide guidance and support to Member States at the national, regional and local level in protecting public spaces. While there can never be ‘zero risk’, these operational measures will help Member States detect threats, reduce the vulnerability of public spaces, mitigate the consequences of a terrorist attack, and improve cooperation.

Following on from the Action Plan, the publication of Good Practices to Support the Protection of Public Spaces (2019) provided the first holistic approach to enhancing the security of public spaces. The best practices were organised around four sections:

1. **Assessment and planning**

1.1. Establish and undertake vulnerability assessments to identify potential vulnerabilities to attack by outsiders or insiders.

1.2. Develop and implement a facility or event security plan, including preparatory, emergency and recovery measures, identifying the appropriate security measures for the facility’s or event’s environment. Security measures need to be effective, discreet, proportionate and tailor-made for different environments I the light of their specific functionality.

1.3. Appoint and train a person responsible for coordinating and implementing the security measures contained in the security plan.

1.4. Develop and implement a crisis management plan.

2. **Awareness and training**

2.1. Initiate public awareness campaigns on reporting suspicious behavior and how to react in the case of an attack which compromises the security of a facility or event.

2.2. Develop and implement an internal security awareness programme for all employees.

2.3. Develop and implement an internal insider threats awareness programme that will help protect facilities or events against different types of insider threats, such as sabotage, commercial theft, or terrorist attacks.

2.4. Develop basic security training programmes for all staff and undertake specific security trainings, contributing to the development of a corporate security culture. Develop activities that motivate employees to implement sound security practices and maintain a high level of security vigilance.

2.5. Undertake regular security exercises that will help identify the level of preparedness to deter and/or respond to an attack.

An important issue to reflect on is the fact that minorities and vulnerable individuals, including persons targeted because of their religion or gender, can be disproportionately affected, and therefore require particular attention.

3. Physical protection

3.1. Assess security and physical protection issues from the beginning of the design process of a new facility or event.

3.2. Assess the necessary access controls and barriers, whilst taking care not to create new vulnerabilities. Access controls and barriers should not shift risks and create new targets.

3.3. Assess the most appropriate detection technology for explosives, firearms, bladed arms, as well as chemical, biological, radiological and nuclear agents.

4. Cooperation

4.1. Appoint contact points and regularly clarify roles and responsibilities in public-private cooperation on security matters (e.g. between operators, private security and law enforcement authorities); this will ensure better communication and cooperation.

4.2. Establish trustful and timely communication and cooperation that allows for a specific risk and threat information exchange between responsible public authorities, local law enforcement and the private sector.

4.3. Coordinate the work on the protection of public spaces at the local, regional and national level and engage in communication and good practice exchanges at all levels, including the EU level.

4.4. Public authorities, together with operators, should develop and make available practical recommendations and guidance materials relating to the detection, mitigation or response to security threats.

The protection of public spaces was an important objective of the EU Security Union Strategy (2020). The emphasis here was on providing both more robust physical protection for such places and adequate detection systems, without undermining citizens' freedoms. The Commission set out to enhance public-private cooperation for the protection of public spaces by means of funding, the exchange of experience and good practices, specific guidance, and recommendations. Awareness raising, performance requirements, the testing of detection equipment, and the enhancing of background checks to address insider threats also form part of the approach. An important issue to reflect on is the fact that minorities and vulnerable individuals, including persons targeted because of their religion or gender, can be disproportionately affected, and therefore require particular attention. Regional and local public authorities have an important role to play in improving the security of public spaces; consequently, the Commission is also helping to foster innovation in the approach municipal authorities take to security in public spaces.

As expected, protection of public spaces and soft targets is an important priority of the EU Counter Terrorism Agenda (2020). The Commission will increase efforts at the EU level to promote security-by-design solutions, which build security into public spaces (buildings and infrastructures) from the very start of the design and urban planning processes. The Commission is committed to enhancing the EU Forum on the protection of public spaces, which collects, consolidates and disseminates knowledge; to supporting the EU Pledge on Urban Security and Resilience; and to using targeted funding to help improve the protection of public spaces. The Commission will also explore the possibility of setting minimum obligations for those responsible for guaranteeing the security of public spaces, which will clarify what is expected from the operators of public spaces.

The Commission will also explore the possibility of setting minimum obligations for those responsible for guaranteeing the security of public spaces, which will clarify what is expected from the operators of public spaces.

Finally, the Council Conclusions on the Protection of Public Spaces (June 2021) provides a list of recommendations and suggestions to both EU institutions and, mainly, the Member States. Among its other recommendations, the Council:

a) Encourages the Commission to continue the efforts it has undertaken in launching and funding initiatives such as the EU Forum for the Protection of Public Spaces, training programmes and projects under the umbrella of the Internal Security Fund and Horizon Europe, and to continue implementing programmes based on volunteer expert peer review.

b) Urges EUROPOL, in line with its legal mandate and in view of the priority-setting mechanisms in place between Member States and the Innovation Lab, to continue exploring digital technologies and measures to counter terrorist attacks in public spaces for the benefit of Member States and every European citizen. This research could focus on developing explosives detection techniques, protecting against unmanned aerial vehicles, tackling serious cybercrime, and using artificial intelligence in the processing of large data sets, in full compliance with the relevant data protection regulations and standards.

Given that Law Enforcement Agencies and private security entities have complementary resources deployed for surveillance, management and communication, effective cooperation between the two would have clear benefits in terms of the protection of European citizens.

c) Encourages Member States to develop, engage with, and actively participate in projects relating to the protection of public spaces and crowded places, creating synergies among international and national stakeholders including regional/local authorities, law enforcement agencies, private security firms and private businesses with the aim of fostering cooperation and the sharing of knowledge that contributes to reducing risks and improving the implementation of smart and safe technologies to protect public spaces.

We can sum up EU approach to the protection of Soft Targets thus:

- Targeted Risk Assessment and Preparedness
- Reinforcing early detection capacity
- Use of novel technologies
- Multi-agency and Public-Private cooperation
- Engage local and regional stakeholders
- Security-by-Design solutions

The APPRAISE Approach and Solutions

Tackling attacks against soft targets requires the collaboration of all stakeholders to achieve real- time holistic situational awareness, predictive competencies, and zero latency intervention. Across Europe, more and more public spaces are owned or operated by private companies and the presence of private guards and security staff is now common. Given that Law Enforcement Agencies and private security entities have complementary resources deployed for surveillance, management and communication, effective cooperation between the two would have clear benefits in terms of the protection of European citizens. Establishing improved operational collaboration among LEAs, private security personnel and citizens has thus become essential.

As the previous section highlights, research and new technologies are important facets of the EU policy for the protection of soft targets. APPRAISE – fAcilitating Public & Private erroris operAtors to mitigate errorism Scenarios against soft targets – is an EU-funded project with an emphasis on soft targets protection. Specifically, APPRAISE will develop and validate a state-of-the-art framework for soft target protection with a particular focus on active, audited and well-defined information plus intelligence exchange among private- and public-sector security practitioners to enable effective collaboration at the information and operational levels.

… the APPRAISE project aims to contribute to this approach and help achieve more effective and efficient proactive operational security for public spaces and soft targets in Europe.

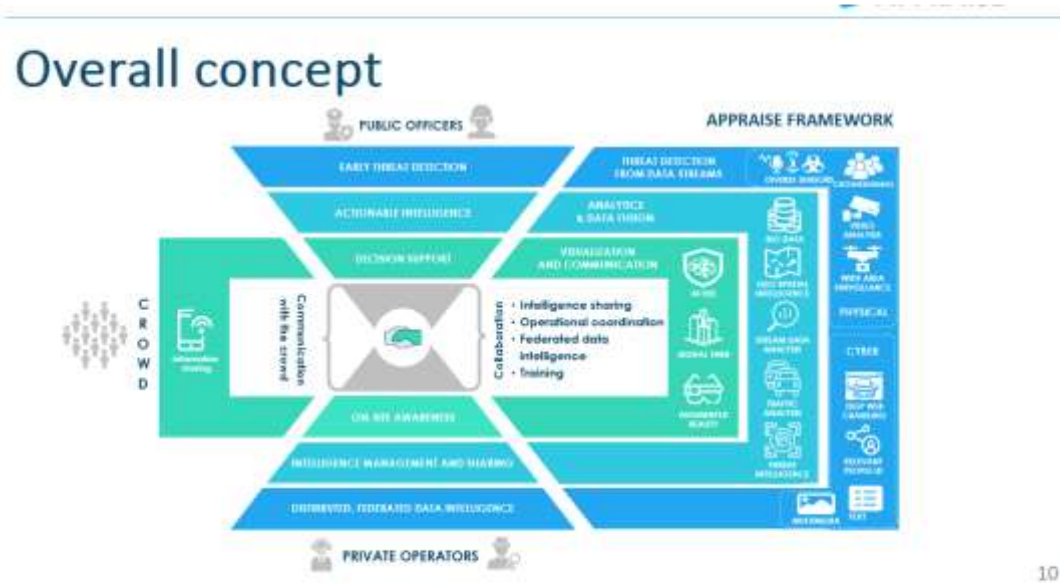

Fig. 2: APPRAISE Architecture

APPRAISE will revolutionize the protection of soft targets by integrating the following:

- A scalable, flexible, and efficient data intelligence platform for threat detection;
- Actionable threat intelligence to proactively detect vulnerabilities and analyse imminent and on-going crimes or terrorist attacks;
- Soft target risk assessments based on web content, social media analysis, and on-site sensor data;
- Instant situational awareness to plan and execute mitigation actions;
- Collaboration capabilities to collaboratively mitigate incidents from the earliest stage of their detection.

Within this framework, the APPRAISE project aims to contribute to this approach and help achieve more effective and efficient proactive operational security for public spaces and soft targets in Europe by:

- Improving the current capability of public and private security practitioners to capitalize on big data information streams.
- Establishing a successful collaboration framework to take advantage of their complementarity in resources.

In line with the EU Policy Framework, APPRAISE contributes to the main pillars of EU policy:

Targeted Risk Assessment and Preparedness

APPRAISE will:

- Parse online sources on the Surface, Deep and Dark web for direct threats and propaganda against soft targets
- Feature the latest advances in AI and Big Data analysis to automatically analyse these online sources for hate speech, to geo-localise the target, and to link the sources to terrorist groups.
- Analyse data from physical sensors to identify threat-related objects and activities in soft targets.
- Develop a risk assessment framework that will combine the above information to assess imminent risks and trigger enhanced preparedness.

Reinforcing Early detection capacity

APPRAISE will:

- Analyse data from physical (fixed and UAV-mounted) sensors to identify threat-related objects such as guns, knives, UAVs and CBRN materials.
- Analyse data streams to identify abnormal events and activities within soft targets, such as gun shots, fighting, and abnormal behaviours and/or densities of traffic/people.
- Feature capabilities to detect cyber-attacks against soft targets.
- Provide actionable threat intelligence to proactively detect vulnerabilities and analyse imminent and on-going crimes or terrorist attacks.
- Utilize a digital twin-based Command and Control system to provide real-time situational awareness.

Multi-agency and Public-Private cooperation

APPRAISE will:

- Enhance Public-Private practitioner cooperation by developing an integrated security approach.
- Facilitate improved communication and information exchange, enabling both parties to seamlessly exchange information when needed.
- Enable operational cooperation enhanced by Augmented Reality glasses for improved communication and information-gathering.
- Facilitate joint training activities for public and private practitioners to streamline their operational efficiency.

Engaging local and regional stakeholders

APPRAISE:

- Will facilitate two-way communication with the public, enabling both information crowdsourcing and guidance during an event through a mobile app.
- Is embracing private stakeholders to utilise their presence and capacity within soft targets.
- Allows information-sharing among all stakeholders through a common information model (need to know access).
- Is building a community to embrace all stakeholders and co-design a commonly acceptable solution.

From the first time, the EU has stated the need to balance the protection of public spaces with respect for privacy, peoples' freedom to move in and use public spaces, and community acceptance of solutions, especially those of a technological nature.

This fundamental pillar of EU policy lies at the heart of APPRAISE project; that is why all the project's solutions are:

- In compliance with GDPR and the EU ethical and privacy framework;
- Acceptable at the societal, community and individual level;
- In compliance with the EU and national legal frameworks;
- Embracing FAIR practices, in the case of Artificial Intelligence solutions.

Policy Proposals

APPAISE is now in the middle of its implementation cycle and crucial activities are ready to be fulfilled in the project's second phase. However, the progress and work of the first phase will allow us to highlight some important points for policy makers at the EU and national level, and to propose specific actions. The proposals relate to i) societal acceptance, ii) the legal framework and privacy issues, and iii) communication and information sharing.

Societal expectations and acceptance of approaches to securing public spaces reveal a high degree of specificity, depending on the type of solution (i.e., technological), type of deployment space, and deployment purpose.

Rapid technological progress means research needs go beyond simple data mining, which is covered by the 2019 Directive on copyright and related rights in the Digital Single Market.

We should therefore:

- Introduce societal concerns into the design and deployment decisions relating to these approaches.
- Consider how to include the public, given that individuals sees themselves as active participants in the creation of security, who are adjacent to – and at times independent of – police or other security actors (e.g., community initiatives, private solutions).

Rapid technological progress means research needs go beyond simple data mining, which is covered by the 2019 Directive on copyright and related rights in the Digital Single Market.

We should therefore:

- Develop centralised data collection and annotation campaigns that can be utilised by research initiatives, as they can significantly boost capabilities.

Testing applications of GDPR-sensitive tools (such as real-time face recognition) is challenging, even in a research setting, due to legal restrictions in force in the Member States.

We should therefore:

- Acknowledge limitations that may stem from the legislative framework in EU-wide and domestic initiatives to promote the protection of soft targets.

Communication and information sharing are crucial, especially during the first moments of an attack on a soft target. However, the market is currently highly fragmented, making interoperability and collaboration exceptionally difficult.

We should therefore:

- Introduce additional standardization initiatives to enable collaboration among multiple agencies and public-private operators.

References

Tony Blair Institute for Global Change, (2018), How Islamist Extremists Target Civilians, Paper, https://www.institute.global/insights/geopolitics-and-security/how-islamist-extremists-target-civilians

Council of the European Union, (2021), Council Conclusions on the Protection of Public Spaces – Council Conclusions (7 June 2021), 9545/21.

European Commission, (2020b), A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final.

European Commission, (2020a), The EU Security Union Strategy, COM(2020) 605 final.

European Commission, (2017a), Fourth progress report towards an effective and genuine Security Union. COM/2017/041 final.

European Commission, (2017), Action Plan to support the protection of public spaces, COM(2017b) 612 final.

M. Fagel- J. Hesterman, (2016), Soft Targets and Crisis Management: What Emergency Planners and Security Professionals Need to Know? New York, Routledge.

JRC, (2022), Security by Design: protection of public spaces from terrorist attacks, Luxembourg: Publications Office of the European Union.

A. Schmid (ed.), (2021), Handbook of Terrorism Prevention and Preparedness, The Hague, ICCT Press Publication, https://www.icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf

T. Zeman, (2020), “Soft Targets: Definition and Identification”, *AARMS*, Vol. 19, No. 1, pp. 109-119.

Project identity

Project name: APPRAISE [Facilitating public & private security operators to mitigate terrorism scenarios against soft targets]

Coordinator: CS GROUP France

Consortium

Participant organisation name	Country
CS GROUP-FRANCE	France
ENGINEERING - INGEGNERIA INFORMATICA SPA	Italy
ITTI SP ZOO	Poland
ALCHERA DATA TECHNOLOGIES LTD	UK
HOLO-INDUSTRIE 4.0 SOFTWARE GMBH	Germany
AITEK SPA	Italy
ETHICAL & LEGAL PLUS SL	Spain
CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS	Greece
FONDAZIONE LINKS	Italy
INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS	Portugal
FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	Spain
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	France
CENTRE OF EXCELLENCE IN TERRORISM, RERILIENCE, INTELLIGENCE & ORGANISED CRIME RESEARCH	UK
HELLENIC FOUNDATION FOR EUROPEAN AND FOREIGN POLICY	Greece
INSTITUTE FOR CORPORATE SECURITY STUDIES LJUBLJANA	Slovenia
POLISH PLATFORM FOR HOMELAND SECURITY	Poland
RECHERCHE, ASSISTANCE, INTERVENTION, DISSUASION	France
COMUNE DI TORINO	Italy
MINISTERIO DA ADMINISTRACAO INTERNA	Portugal
PROVINCIAL POLICE HEADQUARTERS IN GDANSK	Poland
GOBIERNO VASCO - DEPARTAMENTO SEGURIDAD	Spain
MINISTRY OF THE INTERIOR OF THE REPUBLIC OF SLOVENIA	Slovenia
ALTA SEGURIDAD S.A.	Spain
ASOCIACION ORGANIZACIONES CICLISTAS EUSKADI "O.C.E."	Spain
GDANSK INTERNATIONAL FAIR S.A.	Poland
BLAGOVNO TRGOVINSKI CENTER DD	Slovenia
ASTRIAL GmbH	Germany

Funding Scheme: H2020 Innovation action under SU-FCT03-2018-2019-2020**:** Information and data stream management to fight against (cyber)crime and terrorism

Duration: 30 months

Budget: €9,425,581.75

Website: www.appraise-h2020.eu

For more information

Contact Person	Organisation	Email
Yana Lazarova	Project Coordinator	Yana.lazarova@csgroup.eu
Triantafyllos Karatrantos	ELIAMEP	tkaratrantos@eliamep.gr
Eirini Keremidou	ELIAMEP	ekeremidou@eliamep.gr

Further reading:

- Conference paper: 'Securing the smart city: Patterns of public acceptance for integrated technological solutions' - submitted to 2023 IEEE International Smart Cities Conference

Publication expected: To be presented in M25 of the project - Sep 2023

- Journal article: 'What Factors Form Acceptance of Public Space Surveillance? A Systematic Literature Review' - submitted to the Journal of Urban Technology, special issue on 'AI and the City'

Publication expected: Available online as soon as accepted, in print early 2024