APPRAISE

Facilitating public & private security operators to mitigate terrorism scenarios against soft targets

APPRAISE ACHIEVEMENTS

PILOT SUMMARIES AND KEY RESULTS

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement Number 101021981

ABOUT APPRAISE

APPRAISE is an EU H2020-funded project that kicked off in September 2021 with 27 partners from 9 different countries, all coming together to ensure safety in public spaces and protect soft targets from an evolving range of cyber and physical terrorist threats.

Yana Lazarova

CS Group, APPRAISE Project Coordinator

It is a great pleasure to introduce to you this final summary booklet where we'll share information about what APPRAISE has achieved across each of the four pilot sites, the different technologies developed and the important work in addressing and understanding legal and ethical challenges and the acceptance of different technologies by the public and various security actors.

It has been an honour to coordinate APPRAISE through the past two-and-a-half years and to see the dedication and ingenuity of the researchers, end-users, and technology developers who have made it possible.

The protection of public spaces and the resilience of soft targets against physical and cyber threats remains a key priority for the European Union and we hope the achievements within APPRAISE will provide a valuable contribution to the Security Union and capabilities of individual Member States to address such threats.

Aim and Objectives

APPRAISE develops and validates a state-of-the-art framework for soft target protection with a particular focus on active, audited, and well-defined information and intelligence exchange among private and public sector security practitioners to enable effective collaboration at the information and operational levels.

- To ensure the safety of public spaces while preserving the freedom of citizens is a challenge that faces all of society.
- To protect soft targets from an evolving range of cyber and physical terrorist threats.
- To provide an integrated security approach bringing together public and private security operators.

APPRAISE ran four pilots across five different countries ultilising the experience of the local actors and organisations. Each pilot evaluated the technical solutions developed in the project and differs in terms of location, type of event, accessibility, population density, and existing security measures.

APPRAISE

PILOT 1

COORDINATED TERRORIST ATTACK
CROSS-BORDER CYCLE RACE

Pilot organisers

ERTZAINTZA

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

ALSE

POLICE NATIONALE RAID

SCENARIO

In Pilot 1 a cross-border cycle race is targeted by green activists due to the non-environmentally friendly practices of one of the race sponsors. The race starts in the Basque Region of Spain and finishes over the border in France. The scenario requires effective communication between the Basque Police, the private security for the race, and the French SWAT team (RAID) to neutralise the threat.

SCENARIO STEPS

1. Negative sentiment about the race detected on social media as the race begins
2. Several protestors block the area start point while one tries to enter the secure area but flees the scene
3. Aggressive behaviour is detected near the finish line and RAID recieve information from the crowd sensing app
4. A rogue drone is spotted flying overhead which is neutralised and traced to a nearby apartment
5. RAID recieve relevant information and are dispatched to arrest the terrorist

APPRAISE

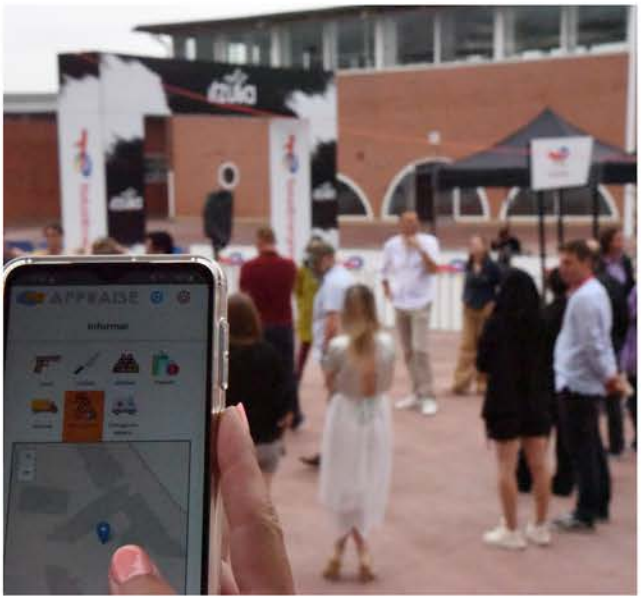
TECHNOLOGIES

The pilot utilises **online content analysis** and **monitoring**, **logo detection and landmark recognition**, **scene text detection and classification** for analysing text and video streams.

All information is aggregated in the **monitoring centre** which also recieved **mobile reports from security and crowd**, while footage is captured from **drone video streams** and the **drone catcher** is deployed. The footage allows for **3D scene reconstruction**

OUTCOMES

The pilot sucessfully tested many elements of the APPRAISE system including the social media monitoring, CCTV analysis, drone patrols over the area, malicious drone detection and pilot localisation and detection of abnormal behaviours from the video stream all brought together through the command and control system.



The emphasis of the pilot was to demonstrate the effective collaboration between the Basque Police, the private security operator and the SWAT team in France (RAID).

The importance of effective cross-border collaboration and sharing of information between organisations was a key achievement for APPRAISE.

APPRAISE

PILOT 2

VEHICLE-RAMMING ATTACK SCENARIO

Pilot organisers

Local Police of Turin

FONDAZIONE links PASSION FOR INNOVATION

SCENARIO

Pilot 2 is a scenario based on a vehicle-ramming attack. It is a simulated event that involves actors from law enforcement, private security operators, and a crowd attending a festival. The scenario took place in the Parco Dora where the annual KappaFutur Festival usually takes place, there were no public participants involved.

SCENARIO STEPS

1. Threats are made against the Festival on social media ahead of the event
2. As people queue, a vehicle rams the crowd and the driver tries to reach the covered area
3. The attacker continues, brandishing a large knife
4. Inside, people try to hide, while some fall and are injured during the escape

APPRAISE

TECHNOLOGIES

The pilot will utilise **online content analysis**, **real-time video analysis** for the identification of logos, weapons and objects, **crowd analytics** and **threat intelligence**

It aslo incoporates reporting and notifications from the **crowd sensing app**, and overall **monitoring and coordination** of the response.

OUTCOMES

Pilot 2 was the final APPRAISE pilot with the opportunity to test the tools at their most mature stage. The project was fortunate to have several members of the press in attendance to publicise the results.

A huge number of APPRAISE technologies were deployed in tandem to carry out the full pilot with attendance from the local stakeholders to enact the scenario.

APPRAISE

PILOT 3

CYBER-PHYSICAL PUBLIC ATTACK SCENARIO

Pilot organisers

SCENARIO

Pilot 3 takes place at the Atlantis Water Park in BTC City in Ljublijana and represents a cyber-physical terrorst attack. Initially, the attack interferes with the SCADA control system and further disrupts the transmission of CCTV images. The complex's private security can share information with the local police and the special police forces after the shooting begins and the attacker takes one of the visitors hostage.

SCENARIO STEPS

1. Unusual posts begin appearing on online and the complex is subject to a cyber attack
2. A person enters the water complex and, once inside, begins shooting the visitors
3. The attacker kidnaps one of the visitors and hostage negotiators arrive
4. Special police enter the complex, rescuing the hostage and arresting the assailant

APPRAISE

TECHNOLOGIES

The pilot utilised online monitoring and hate speech detection, audio detection, anomaly detection and analysis from CCTV video streams

The pilot also used the monitoring centre and the **crowd sensing app**, as well as threat object detection and threat intellingence for the detecting the cyber attack

OUTCOMES

Pilot 3 was the first pilot run by APPRAISE and was coupled with the national annual exercise of the Slovenian Police.

Both public and private security operators were involved, as well as the National Police, SWAT team and other local partners. More than 20 stakeholders were attendance to see the demonstration which was supported by several volunteers.

The pilot was able to test new procedural and technological approaches in a real environment in a real-time scenario.

The exercise demonstrated the applicability of the process and technology approaches developed so far within APPRAISE and provided a quality basis for further development and testing of these approaches in the forthcoming three pilots within the project.

APPRAISE

PILOT 4

COLD-WEAPON ATTACK SCENARIO

Pilot organisers

Polish Platform For Homeland Security

amber expo

POLICJA

SCENARIO

Pilot 4 is a cold-weapon attack scenario. It is a simulated event that involves actors from law enforcement, private security operators, and a crowd. The scenario took place after the TRAKO fair has ended, so there were no public participants involved.

SCENARIO STEPS

Prior to the event, hateful and threatening messages relating to the event are found on social media.

A cyber attack starts against the official website. A person enters the TRAKO fair with a cold weapon and begins to attack the attendees.

The rapid and violent attack causes panic, which requires effective management from the crowd and evacuation to avoid additional victims.

As a result, participants who are escaping are hurt or went into hiding

APPRAISE

TECHNOLOGIES

The pilot will utilise **online content analysis**, **cyber attack detection**, **real-time video analysis** for the identification of weapons and objects, and **drone-based area surveillance**.

Through a **crowd sensing app** participants inform AmberExpo security officials that a potentially dangerous event is taking place while participants also receive instructions from the LEA.

OUTCOMES

It was the first pilot that took place in a real environment during an ongoing event. This gave the consortium a unique opportunity to test the APPRAISE solution in a real environment during the TRAKO fair.

Pilot 4 proved that the technologies developed within APPRAISE work in real conditions during a public event.

The exercise served as a way to better cooperation between public and private security operators in the field of protection of public spaces in the event of attacks.

The pilot involved public and private security forces and volunteers from the Naval Academy of the Heroes of Westerplatte, who enabled us to demonstrate the APPRAISE tools to more than 20 stakeholders.

The stakeholders had a chance to interact with the technological partners and ask questions related to each specific tool during an open carousel session.

APPRAISE

APPRAISE
TOOLS

ONLINE DATA ACQUISITION & **TEXT ANALYSIS**

Web Search

CERTH

Web search enables the submission of keyword-based queries to search engines, both on the Surface (e.g., Google and DuckDuckGo) and Dark Web (e.g., Ahmia and Torch). The tool merges the returned results (i.e., web pages) and removes the duplicates. Next, the textual and media content of each web page is downloaded.

Social Media Crawler

CERTH

The social media crawler supports the continuous monitoring of Twitter, which employs two modalities of discovery: (i) keyword-based search, where content relevant to a query is returned, and (ii) account-based search, where content posted from this account is returned.

The tool uses the official Twitter API and complies with the Terms of Service. Personal data (e.g., IDs and usernames) are encrypted for anonymisation purposes.

Hateful Speech Detection

LINKS

The hate speech detection module can identify hateful users by analysing a graph of user interactions and relationships within social media. It uses advanced Natural Language Processing approaches to create user representations in an embedding space. It performs hateful detection through a complex graph neural network analysis, which considers the user activity and the content generated by similar users.

Web Crawler

CERTH

The web crawler gathers data from the surface and dark web by traversing the hyperlink structure of the web, starting from a set of given seed URLs.

Targeted Extraction

CENTRIC

Targeted extraction improves the quality of results from web crawling by ensuring that only the main content the post structure of web page is extracted and all extraneous information such as menus and adverts are excluded.

Text Analysis

CENTRIC & VICOM

The text analysis module provides a variety of text processing and analytical operations. The module enriches existing text through entity extraction, provides text summarisation to give a shortened text summary of a given input text, performs keyword extraction, sentiment and subjectivity analysis to determine the polarity and extent to which the text is based on an opinion.

CROWD BEHAVIOUR **ANALYSIS**

Crowd Analysis Tool

LINKS

The crowd analysis tool allows APPRAISE to monitor gatherings by estimating pedestrian flows to identify clusters and extract descriptive analytics. It monitors crowded scenarios, delivering crowd metrics (e.g., counter of people, crowd density, crowd heatmaps), estimating the pedestrian flow direction and speed, and raising alerts on specific circumstances (e.g., increasing speed of pedestrians, crowd running, panic) to support LEAs in decision making.

Crowd Prediction Tool

CERTH

The crowd prediction tool allows the user to predict the number of people in an area after a set time step using the crowd analysis tool's output. The model is trained on synthetic data generated from a simulated environment comparable to the actual area. The crowd's attendance depends on different parameters such as the type of venue, time of day, weekday or weekend.

Panic Detection Tool

VICOM

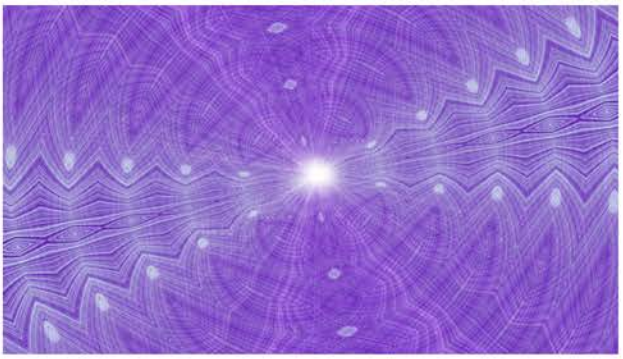
The panic detection tool distinguishes between panic and normal situations. A panic situation is where people start running away from danger. The tool primarily works with large crowds in outdoor environments. However, for the pilot phase, it is being adjusted to be used with smaller crowds in indoor environments.

AUDIO AND SENSOR **ANALYSIS**

Audio Surveillance

CEA

The audio surveillance tool implements the audio scene analysis system for detecting relevant events, such as screaming, fighting, gunshots or glass breaking.



Audio Event Detection

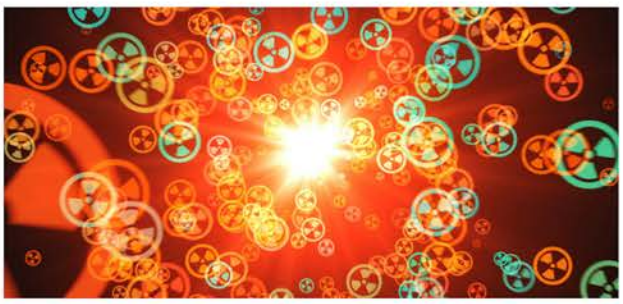
ASTRIAL

The Audio Event Detection module detects events from different sensors and is focused on the detection and spatial localisation of abnormal/terrorism related activities using audio sensors, i.e., array of microphones.

Gamma Camera Tool

CEA

this tool is related to the implementation of a system that is able to track potential radiological and nuclear threats using a specific sensor, called gamma camera. Additionally, infrared sensors allow it to operate in dark environments.



Automatic Speech Recognition and Keyword Spotting

VICOM

Using an audio file, language and a list of target keywords, the audio file can be transcribed and the user is provided with the timestamps of when the different keywords appear in the spoken text.

APPRAISE

MULTIMEDIA ANALYSIS

Multimedia Content Criminal Indicator Detection

CERTH

It comprises a set of tools for detecting logos of UN-sanctioned terrorist groups and recognising significant landmarks. Using data from the crawler assists in discovering possible relations between suspicious posts, possible attacks, their targets and the related terrorist groups.

Threat Related Object Detection

CERTH

The object detection tool uses continuous real-time monitoring of CCTV footage to detect threat-related objects such as guns, knives and backpacks, allowing LEAs to react instantly and prevent possible attacks in public places and events.

Scene Recognition

VICOM

The Scene Recognition Tool takes an image and predicts the category of the place pictured. It can classify the image into one of 38 categories, such as a park or a shop. Additionally, it can predict the coordinates of the image. The tool only uses the image to make these predictions and it is trained to work with a large number of images.

Scene Text Detection

VICOM

The Scene Text Detection Tool can extract text from images. It can identify and localise text within natural images or videos, such as street signs, billboards, or posters. Other modules can use the extracted text to find relevant clues for investigations.

Mobility Anomaly Detection

ALCHERA

The anomaly detection tool monitors road vehicle traffic in real-time. It identifies anomalous conditions, such as unexpected traffic build-up, and reports traffic conditions and incidents from various data providers. The tool quickly identifies accidents on the road to reduce the time to discovery and intervention of emergency services.

Anomaly Event Detection

CERTH

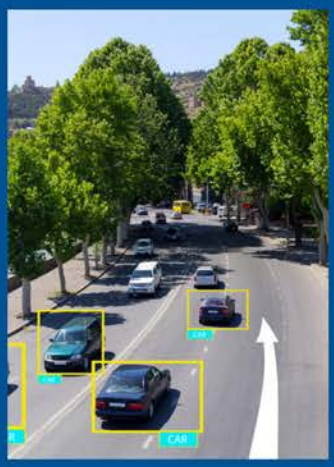
The anomaly event detection provides continuous real-time monitoring using CCTV footage in order to detect possible abnormal events, such as fights or arson, and enables authorities to react instantly and prevent possible damage, injuries or further casualties in public places and events.

APPRAISE

AiVu - Video Surveillance

AITEK

The video surveillance platform offers a wide range of innovative technologies for image acquisition and processing. It includes: NVR devices (for the acquisition, recording and distribution of video streams), the VMS (an application offering a centralized interface for the management of an entire CCTV system), and the Smart Modules (video analytics). These devices are highly scalable and can be used to create CCTV networks of any size (from a single camera to thousands), and can be deployed on premise, on the cloud or even hybridly (partly on premise and partly on the cloud). The Smart Modules offer a wide variety of tools, including the ability to detect when the video camera has been tampered with (such as being covered, obscured, or rotated away from its typical position).



AiVu - Smart Modules

AITEK

Video analytics software developed by Aitek that can process video footage and images and generate alarms appropriately. Its tools include: detecting people in video streams, monitoring specific areas for intrusions or crowds, monitoring the direction and speed of travel of vehicles, and detecting people that have fallen or are laying on the ground. Finally, the Smart Modules can compute the embedding of every person or vehicle that it detects: this is a feature vector that can be used to efficiently match and track targets in a multi-camera system, including finding the same target in different cameras and at different times (i.e. in the recordings).

Landmark Recognition

CERTH

The Landmark Recognition tool is able to detect well-known landmarks that appear in images.

Backpack Detection

CERTH

The Backpack Detection tool takes video input from real-time video streams and is able detect the appearance of a backpack. It outputs both the timestamps for the appearance of the backpack as well as the coordinates for a bounding box around the backpack.

Propaganda Detection

CERTH

The propaganda detection tool detects content related to propaganda - specifically Jihadi content - in video streams.

UAV SYSTEMS

Drone-based Wide Area Surveillance

ASTRIAL

A drone-based wide-area surveillance platform consists of a high-end DJI M350 RTK drone that allows for a 2.7 kg payload and up to 55 minutes of surveillance of an infrastructure. The drone is controlled via a Ground Control Station and allows live streaming of the aerial imagery captured and the execution of the object detection, together with the object localisation and tracking functionalities. This innovative surveillance technology offers the following benefits and advances the state-of-the-art in the following aspects:

- Easily customisable real-time streaming of the surveillance area to a variety of external platforms (such as DITHO) with the use of video management platforms.
- High accuracy and confidence in detecting abnormal activity by persons and vehicles within a 2x2 km surveillance area exploiting a variety of threat profiles.
- Real-time, semi-autonomous localisation and tracking of the objects performing the abnormal activity.
- Quick generation of updated 3D models of the surveilled area that can be geo-referenced and visualised in standard mapping environments allows simultaneously adding layers of information in a geo-referenced manner, hence boosting situational awareness.
- Increased safety and security of the soft target under surveillance.

Counter UAV System

CS

The CUAS developed by CS GROUP within APPRAISE, which is based on the solid foundations of the Boreades product, aims at protecting sensitive sites, infrastructures and public spaces. The system can detect a drone of any size and its manufacturer, and it offers a comprehensive solution ranging from the definition of a no-fly-zone, to drones detection, identification classification, and neutralisation. Connected to the APPRAISE Hypervision system (DITHO), security operators can overview and share the tactical situation including the drones' tracks localised on a map of the environment, as well as the drone's remote control positions, thus enabling responders to quickly assess the situation and plan for possible neutralisation.

The multiple system configurations, fixed, portable or mobile, make it a valuable asset to protect various environments such as sensitive sites, critical infrastructures and public spaces from the constantly increasing and evolving unmanned aerial threat.

APPRAISE

INTELLIGENCE & **MONITORING**

Threat Intelligence Tool

ENG

The Threat Intelligence Tool (ThINT) has two main goals. The first is related to data fusion techniques to aggregate and fuse data from live sensors (i.e., reports sent by citizens with the crowd app, detected input from microphones or cameras). Data fusion is the process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source. For this reason, raw data from the sensors are collected and aggregated to produce more accurate alerts for end-users.

The second goal is to apply threat intelligence in social networks and the deep and dark web to identify potential menaces to soft targets. Sharing material on social media, blogs, and forums has been increasingly valuable in recent years as social networks have grown in popularity for tracking down and identifying potentially dangerous content. For this reason, the scope of our framework is to use state-of-the-art techniques to identify and classify threats from social networks and the deep and dark web.

MARPLE

ENG

MARPLE, because of the famous Miss Marple (a fictional character in Agatha Christie's crime novels and short stories), represents a Graphical User Interface (GUI) that allows the end-user to access different services related to background tools.

For example, from the **MARPLE Monitoring**, it is possible to access the monitoring of social networks by defining the keywords used by the crawlers. From the **Marple Intelligence**, it is possible to visualise all the threats identified by Threat Intelligence, with all the details of a recognised threat (for example, a video attached, the list of social posts recognised, etc.). The last application is **Marple Vision**, which allows the visualisation of specific detections from previous videos (i.e., weapons, objects, events). It also supports tracking a person of interest receiving alerts when that person is recognised in another camera, and searching for a person of interest in previous videos (namely re-identification).

APPRAISE

Cyber and Network Attack Detection

ITTI

The Network Intrusion Detection Component developed by ITTI utilises machine learning techniques for cyberattack detection. The tool analyses network traffic with advanced learning algorithms, with the results of the detection presented as user-friendly visualisations in an informative dashboard, The Network Intrusion Detection Component is a versatile, scalable, and intelligent system for adept real-time network security analysis.

Emergency Evacuation Optimisation

CERTH

The Emergency Evacuation Optimisation leverages artificial intelligence based on Reinforcement Learning algorithms and is able to allocate people/civilians to emergency exits based on the following parameters: site structure and available exits, number of people and their local distribution in the site, emergency event type and location. Additionally, the inclusion of a simulation component allows users to experiment with different evacuation scenarios, fostering a deeper understanding of optimal strategies. Ultimately, this serves to empower authorities and individuals with advanced, data-driven insights, enabling them to make well-informed decisions during critical situations and contributing to improved public safety and emergency response capabilities.

APPRAISE

Augmented Reality Situational Awareness

HOLOLIGHT

The Augmented Reality (AR) Smart Glasses enhance human-machine interaction and improve situational awareness in critical security scenarios. This enables security operators to make quicker and more effective decisions, coordinate operations more efficiently, and share information. EVA (Enhanced Vision App) is a bi-directional system, which allows an operator wearing HL2 to view holographic data overlaid on the real world, such as:

- image, geo location of suspect,
- results from image/object recognition software,
- mini map and directional indicators, and
- other relevant data captured by other tools.

In return, the camera feed from the HL2 are being transmitted back, giving remote operators a better view of the incident site.

Collaborative AR Training

HOLOLIGHT

The collaborative augmented reality training provides a tool to support training in a realistic environment. The aim of this technology is to increase the efficiency, safety, and preparedness of security operators. The application that uses holograms to create dynamic training. Augmented Reality and Real-Time Object Tracking allows for the same training settings to be used in multiple locations.

It offers a customised-training mode with options for speed, accuracy, perception, reaction and bias training. Different transitions, animations, and states for avatars (terrorists, hostages, and friendly people) are included.

Geo-spatio-temporal Complex Event Processing Engine (GCEP)

ASTRIAL

Geo-spatio-temporal Complex Event Processing Engine (GCEP) is a complex event processing engine that allows the input of a multitude of low-level threat alerts detected and identified by the sensing tools of the APPRAISE ecosystem and, in turn, correlates them according to user-configurable spatio-temporal rules and outputs higher-level alerts that are pushed to a map-based visualisation platform.

The correlation rules implemented in GCEP include:

- Location (polygon) - the user defines the area of the alerts.
- Time (interval) - the user defines the time interval for the alerts.
- Sensing input (type of detection and selection of sensor ID) - the user defines which sensors are to be considered.
- Confidence level (% reliability of the result) - the user defines which range of reliability is useful.

Geo-spatial intelligence technology provides high-speed event processing and identification of the most significant events from within a plethora of events. Complex Event Processing (CEP) patterns result from relationships between event attributes, time, cause (causal relationship between events), and aggregation (the importance of the activity of one event over other events).

Spatial relationships are used to combine location-based events and generate spatio-temporal patterns. GCEP provides actionable information to LEA operators.

Intelligent Hypervision and Operation Management for Soft Target Protection

CS Group France

The APPRAISE Operation Management System, named the DITHO (Digital Twin based Hypervision and Operations Management system), enables the visualization of the situation and management of the ongoing operations, aggregating multiple sources of information such as maps, 3D representation of buildings, surveillance cameras, first responders locations, drones and sensor alerts and to provide novel decision making capabilities powered by AI-assisted processing.

Moreover, the DITHO has been designed to foster the collaboration between LEAs and private security operators and improve responsiveness and effectiveness of the operations. For this purpose, the DITHO can be deployed on multiple devices, including tablets and mobile phones, thus facilitating the exchange of information between the different security operators, as well as between the command and control centre and the agents deployed on the scene.

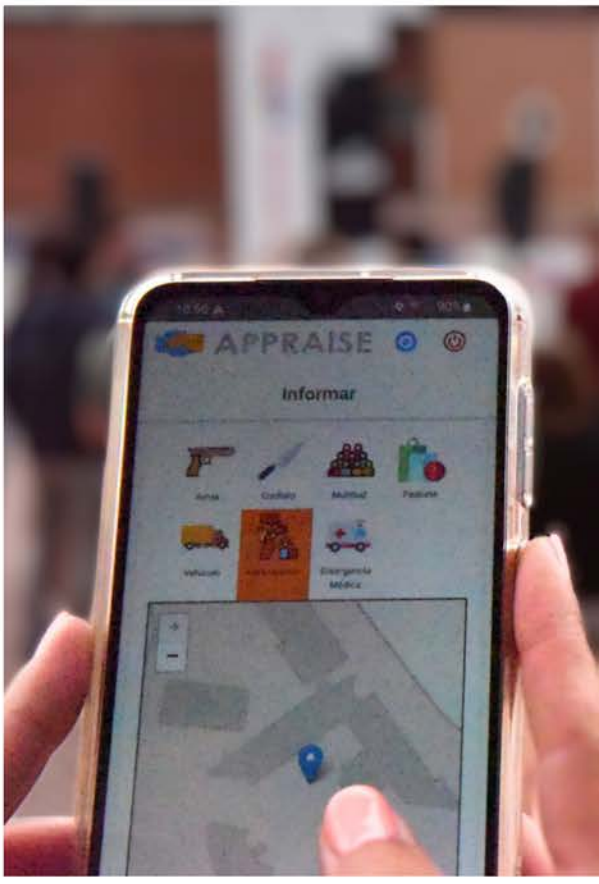
Crowd-sensing Framework

INOV

The Crowdsensing Framework is divided into two main tools. The first one is a **Crowdsensing Dashboard**, that is integrated in DITHO, that allows the LEA operators to receive and perceive information from the crowd by allowing the accurate visualisation of the amount of users in the crowd and the anomalies reported and their respective locations in a map of a given event.

This helps make informed decisions regarding the crowd and how certain occurrences during an event are handled by the crowd. The Dashboard also provides the ability for rapid communication with the event users, by allowing LEAs to send messages directly to their mobile devices.

The second tool is a **Crowdsensing Mobile Application**, to be used by the participants of an event that allows them to quickly communicate with the LEAs by being able to report anomalies with descriptions and photos. They are also able to receive personalised security instructions in case of an emergency as well as general event information.



APPRAISE
RESEARCH

Legal & Ethics

PLUS ETHICS

A comprehensive analysis and monitoring of the ethical/privacy risks associated with the project's tasks, together with recommendations to mitigate these risks and ensure compliance with EU ethical standards.

The reports detailed the project's compliance with ethical principles and data protection and assessed how ethical objectives, including privacy and data integrity, were achieved throughout the project. They also included a retrospective analysis to identify and manage potential ethical risks, an assessment of compliance with European ethical/legal standards, and a review of the mechanisms for assigning ethical/privacy responsibilities.

The aim of this assessment was to ensure transparency, accountability and sustainability in the management of ethical and privacy issues within the project and to minimise negative impacts on communities and stakeholders.

Ethics and Cybersecurity

ITTI

As part of APPRAISE ethics work ITTI completed a wide-ranging horizon-scanning campaign on the upcoming ethical dilemmas in cybersecurity. This study has been successfully published in a prestigious scientific journal: "Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, M. (2023). What will the future of cybersecurity bring us, and will it be ethical? The hunt for the black swans of cybersecurity ethics. IEEE Access."

Societal Acceptance

CENTRIC

CENTRIC investigated the societal acceptance of the APPRAISE approach to public space protection, using a mixture of desk-based research, surveys, and focus groups to engage with a broad set of societal actors across seven APPRAISE partner countries.

The combined qualitative and quantitative result show a considerable societal acceptance of the individual technology solutions developed by APPRAISE and their deployment in concrete situations. In addition, the research offers insights into societal concerns and concrete requests for safeguards such as appropriate controls, adequate regulation and clearly defined usage purposes.

Together, the findings help inform communications with citizens as well as technological and policy development.

Policy Analysis

ELIAMEP

ELIAMEP produceed a policy paper titled 'Protecting Soft Targets from Terrorist Attacks - Security and Foreign Policy'. The outcomes of the research included:

- 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.

APPRAISE

JOIN THE APPRAISE **COMMUNITY**

If you work in the areas of the protection of public spaces, law enforcement, first responders, or private security, APPRAISE needs your knowledge and expertise.

Join our online community and create a direct impact on the research outcomes of the project plus much more!

Email us at appraise-h2020@csgroup.eu to get involved.

CONTACT US

appraise-h2020@csgroup.eu

appraise-h2020.eu

SOCIAL MEDIA

appraise_h2020

appraise-project

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement Number 101021981.

APPRAISE Partners

This project has received funding from the European Union's Horizon 2020 programme under grant agreement No. 101021981.

APPRAISE

Facilitating public & private security operators to mitigate terrorism scenarios against soft targets