Data analytics and AI bias in LEAs decision-making

Challenges, gaps and related innovation solutions

19.05.2023 10:00 AM - 12:00 PM CET

NOTIONES + popAI | ALLIES

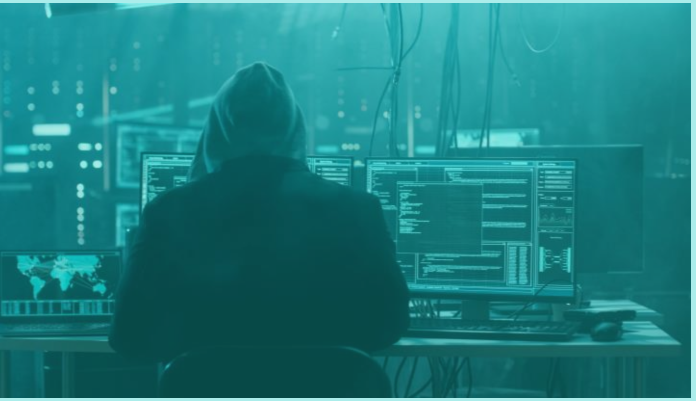
Host: SYNYO GmbH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Agenda

Time	Topic	Presenter
10:00 - 10:05	**Introduction to the webinar and expected results**	**Alexander Nikolov** SYNYO GmbH, Austria
10:05 - 10:20	**NOTIONES project**	**Alexander Nikolov** SYNYO GmbH, Austria
10:20 - 10:35	**popAI project**	**Dr Dimitris M. Kyriazanos, Project Coordinator** NCSR Demokritos, Greece
	Use cases	
10:35 - 10:50	**Greek policy lab**	**Anthoula Bania** Hellenic Police, Greece
10:50 - 11:05	**German policy lab**	**Pinelopi Troullinou** Trilateral Research, Ireland
11:05 - 11:20	**Slovak policy lab**	**Mojmír Mamojka** Academy of the Police Force in Bratislava, Slovakia
11:20 - 11:35	*Round table discussion*	
11:35 - 11:45	**ALLIES project**	**Denitsa Kozhuharova** Law and Internet Foundation, Bulgaria
11:45 - 11:55	**LAW-GAME project**	**John Soldatos** INNOV-ACTS LIMITED, Cyprus
11:55 - 12:05	**STARLIGHT project**	**Ezgi Eren** KU Leuven Centre for IT & IP Law – imec, Belgium
12:05 - 12:10	**Final remarks**	**Alexander Nikolov** SYNYO GmbH, Austria

HOUSEKEEPING RULES



NOTIONES

The session will be entirely recorded and published on the NOTIONES project website.

All participants except speakers and moderators will be **muted by default**.

Feel free to post your questionsions in the **chat**.

If you would like to speak, raise your hand and wait for the moderator to give you the floor.

PROJECT OVERVIEW

Acronym:	NOTIONES
Title:	iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS
Duration:	01.09.2021 – 31.08.2026
Topic:	SU-GM01-2020
Call:	Pan-European networks of practitioners & other actors in the field of security
Funding:	H2020
Type:	Coordination and Support Action (CSA)
GA Number:	101021853
Coordinator:	Fundacion Tecnalia Research & Innovation
Consortium:	30 Partners
Website:	www.notiones.eu
Cordis:	CORDIS Project Profile

OVERVIEW

CONSORTIUM

Fundadcion Tecnalia Research and Innovation (TECNALIA)

Spain

Zanasi & Partners (Z&P)

Italy

Laura-Ammattikorkeakoulu (LAU)

Finland

Institut Po Otbrana (BDI)

Bulgaria

Defence Research Institute (DRI)

France

Intelligence Culture and Strategic Analysis (ICSA)

Italy

Bar-Ilan University (BIU)

Israel

Agenzia Per La Promozione Della Ricerca Europea (APRE)

Italy

Teknologian Tutkimuskeskus Vtt OY (VTT)

Finland

Expert System SPA (EXPSYS)

Italy

SAHER (SAHER)

Estonia

MarketScape

Denmark

TECOMS SRL (TECOMS)

Italy

SYNYO GmbH

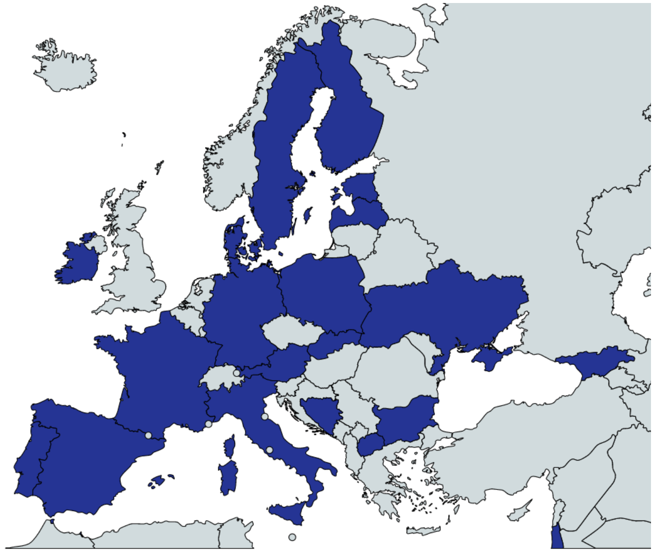
Austria

Masovian Police (KWPR)

Poland

DURZHAVNA AGENTSIYA NATSIONALNA SIGURNOST (DANS)

Bulgaria



LESO LEONARDO (LL)

Italy

Financial Intelligence Unit

Financial Intelligence Unit Latvia (FIU)

Latvia

Beyond the Horizon International Strategic Studies Group (BtH)

Belgium

International Security and Emergency Management Institute (ISEM)

Slovakia

Kharkiv National University of Internal Affairs (KhNUIA)

Ukraine

Estonian Police and Border Guard Board

Politsei- ja Piirivalveamet

Estonia

Ministry Of Internal Affairs (MIA)

Georgia

Police Service of Northern Ireland (PSNI)

Ireland

POLISMYNDIGHETEN SWEDISH POLICE AUTHORITY (SPA)

Sweden

Ministério da Justiça (PJ)

Portugal

Military Academy Skopje (MAGMA)

North Macedonia

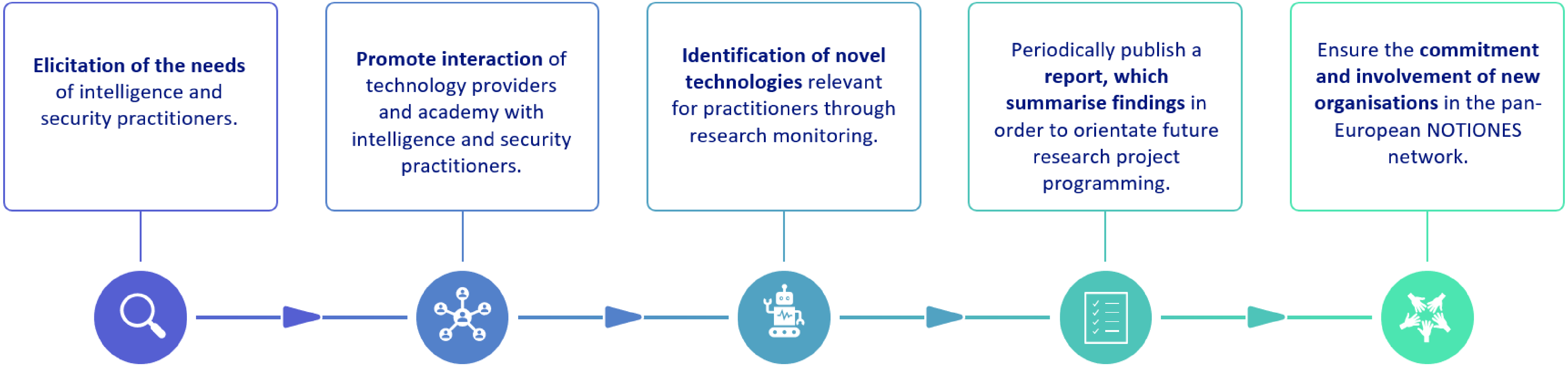
HOCHSCHULE FUR DEN ÖFFENTLICHEN DIENST IN BAYERN (HföD)

Germany

Ertzaintza (ERTZ)

Spain

KEY OBJECTIVES



Elicitation of the needs of intelligence and security practitioners.

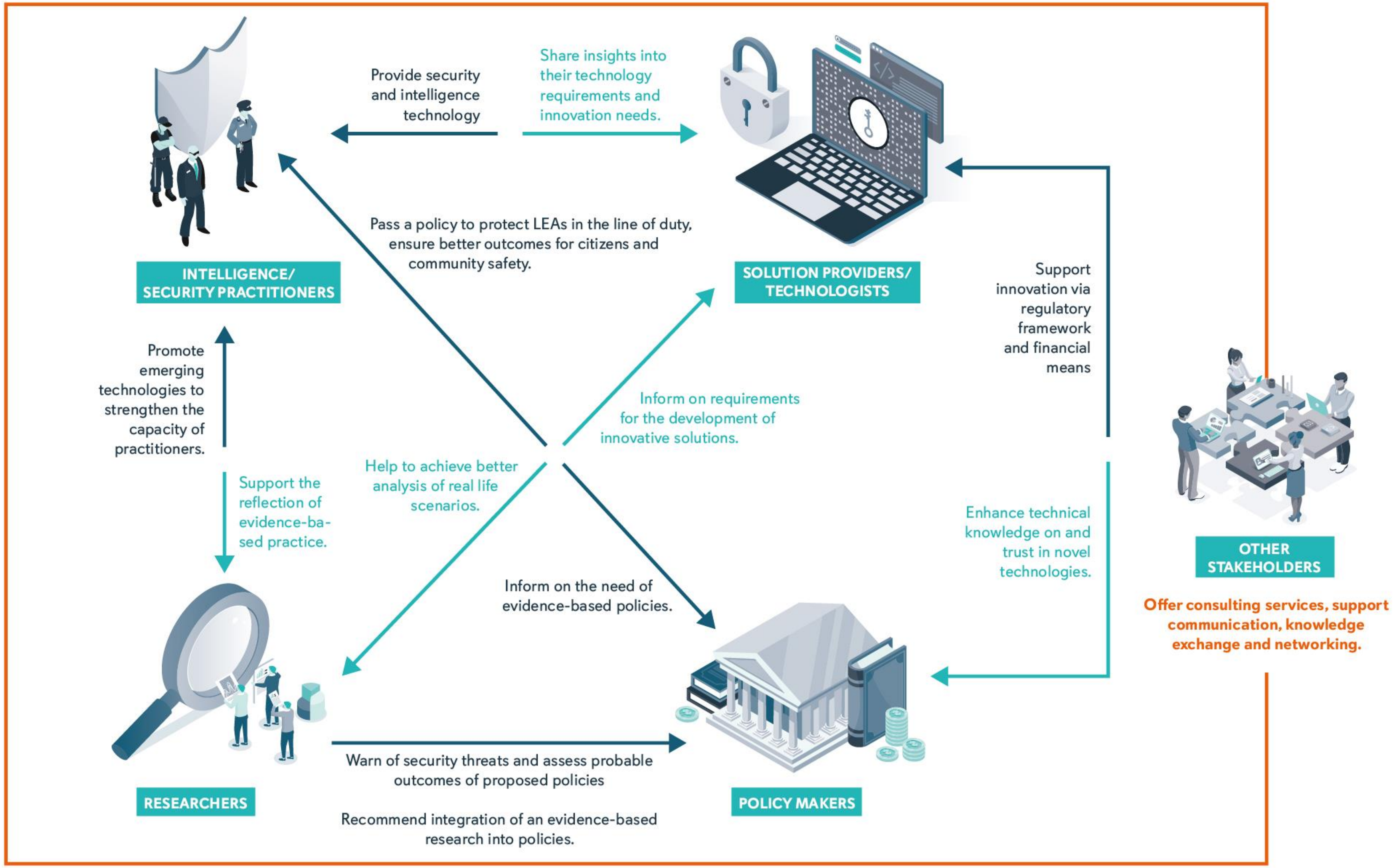
Promote interaction of technology providers and academy with intelligence and security practitioners.

Identification of novel technologies relevant for practitioners through research monitoring.

Periodically publish a **report, which summarise findings** in order to orientate future research project programming.

Ensure the **commitment and involvement of new organisations** in the pan-European NOTIONES network.

NOTIONES NETWORK



INTELLIGENCE/ SECURITY PRACTITIONERS

Provide security and intelligence technology

Share insights into their technology requirements and innovation needs.

SOLUTION PROVIDERS/ TECHNOLOGISTS

Pass a policy to protect LEAs in the line of duty, ensure better outcomes for citizens and community safety.

Promote emerging technologies to strengthen the capacity of practitioners.

Support the reflection of evidence-based practice.

Inform on requirements for the development of innovative solutions.

Help to achieve better analysis of real life scenarios.

Inform on the need of evidence-based policies.

Support innovation via regulatory framework and financial means

Enhance technical knowledge on and trust in novel technologies.

OTHER STAKEHOLDERS

Offer consulting services, support communication, knowledge exchange and networking.

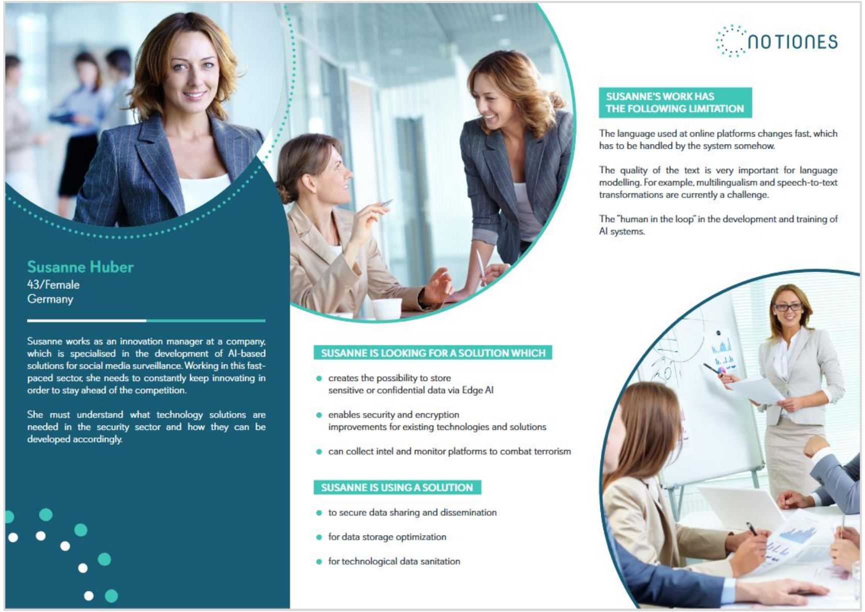
RESEARCHERS

Warn of security threats and assess probable outcomes of proposed policies

Recommend integration of an evidence-based research into policies.

POLICY MAKERS

NOTIONES PERSONAS



Susanne Huber

43/Female
Germany

Susanne works as an innovation manager at a company, which is specialised in the development of AI-based solutions for social media surveillance. Working in this fast-paced sector, she needs to constantly keep innovating in order to stay ahead of the competition.

She must understand what technology solutions are needed in the security sector and how they can be developed accordingly.

SUSANNE'S WORK HAS THE FOLLOWING LIMITATION

The language used at online platforms changes fast, which has to be handled by the system somehow.

The quality of the text is very important for language modelling. For example, multilingualism and speech-to-text transformations are currently a challenge.

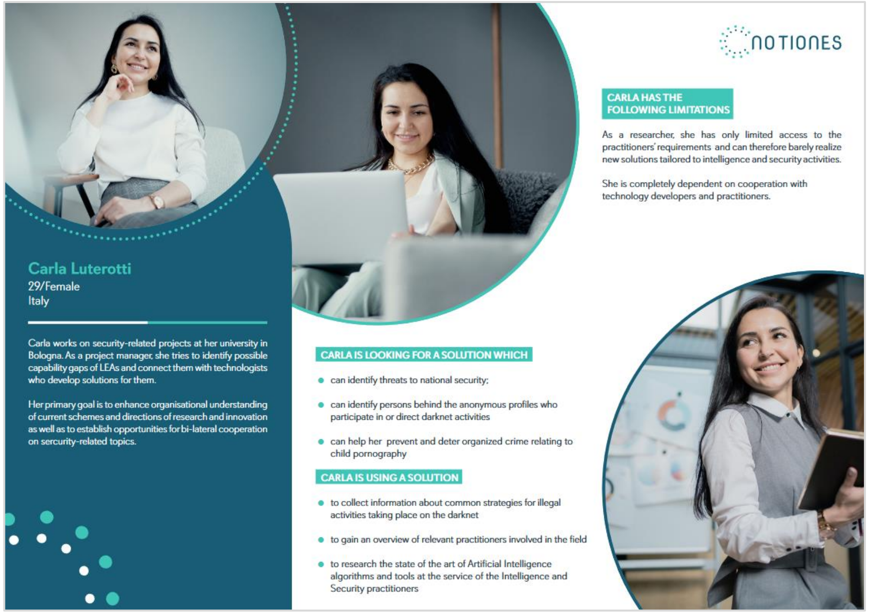
The "human in the loop" in the development and training of AI systems.

SUSANNE IS LOOKING FOR A SOLUTION WHICH

- creates the possibility to store sensitive or confidential data via Edge AI
- enables security and encryption improvements for existing technologies and solutions
- can collect intel and monitor platforms to combat terrorism

SUSANNE IS USING A SOLUTION

- to secure data sharing and dissemination
- for data storage optimization
- for technological data sanitation



Carla Luterotti

29/Female
Italy

Carla works on security-related projects at her university in Bologna. As a project manager, she tries to identify possible capability gaps of LEAs and connect them with technologists who develop solutions for them.

Her primary goal is to enhance organisational understanding of current schemes and directions of research and innovation as well as to establish opportunities for bi-lateral cooperation on sercurity-related topics.

CARLA HAS THE FOLLOWING LIMITATIONS

As a researcher, she has only limited access to the practitioners' requirements and can therefore barely realize new solutions tailored to intelligence and security activities.

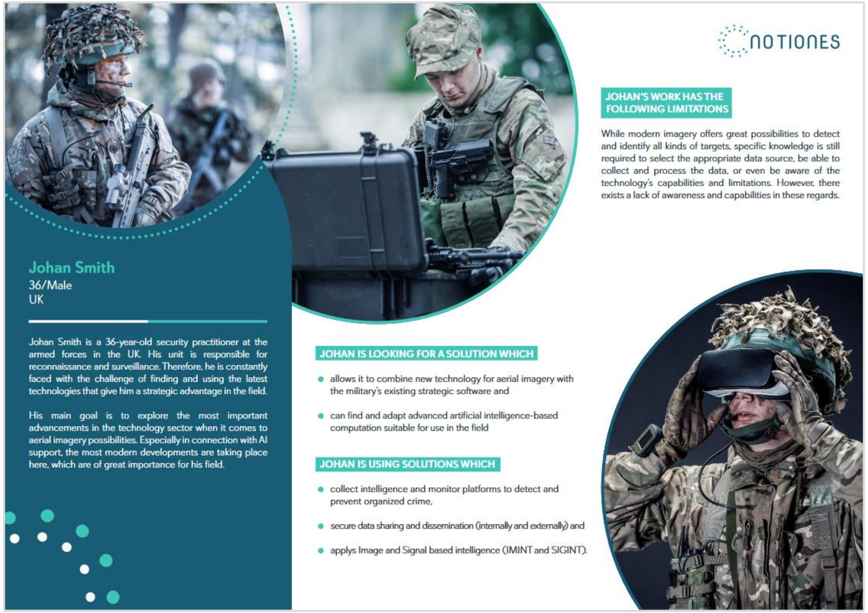
She is completely dependent on cooperation with technology developers and practitioners.

CARLA IS LOOKING FOR A SOLUTION WHICH

- can identify threats to national security;
- can identify persons behind the anonymous profiles who participate in or direct darknet activities
- can help her prevent and deter organized crime relating to child pornography

CARLA IS USING A SOLUTION

- to collect information about common strategies for illegal activities taking place on the darknet
- to gain an overview of relevant practitioners involved in the field
- to research the state of the art of Artificial Intelligence algorithms and tools at the service of the Intelligence and Security practitioners



Johan Smith

36/Male
UK

Johan Smith is a 36-year-old security practitioner at the armed forces in the UK. His unit is responsible for reconnaissance and surveillance. Therefore, he is constantly faced with the challenge of finding and using the latest technologies that give him a strategic advantage in the field.

His main goal is to explore the most important advancements in the technology sector when it comes to aerial imagery possibilities. Especially in connection with AI support, the most modern developments are taking place here, which are of great importance for his field.

JOHAN'S WORK HAS THE FOLLOWING LIMITATIONS

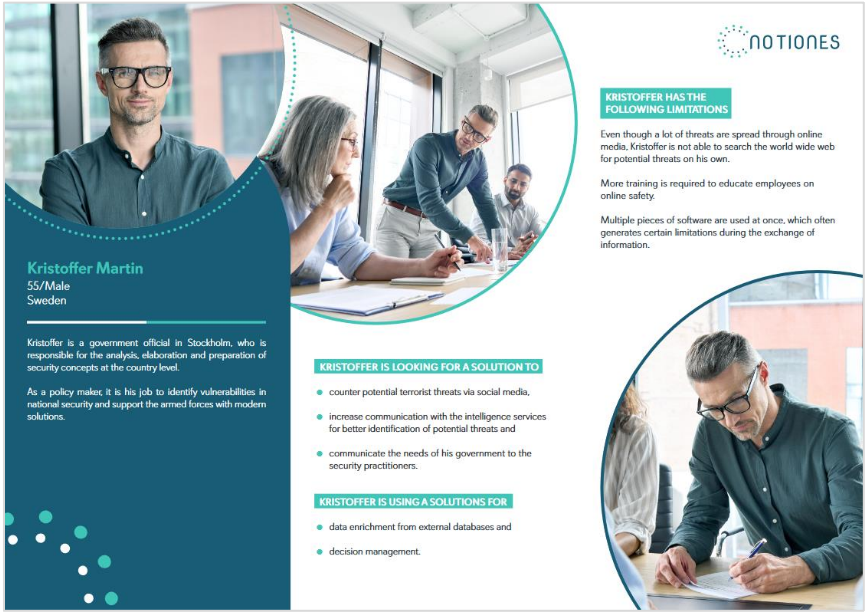
While modern imagery offers great possibilities to detect and identify all kinds of targets, specific knowledge is still required to select the appropriate data source, be able to collect and process the data, or even be aware of the technology's capabilities and limitations. However, there exists a lack of awareness and capabilities in these regards.

JOHAN IS LOOKING FOR A SOLUTION WHICH

- allows it to combine new technology for aerial imagery with the military's existing strategic software and
- can find and adapt advanced artificial intelligence-based computation suitable for use in the field

JOHAN IS USING SOLUTIONS WHICH

- collect intelligence and monitor platforms to detect and prevent organized crime,
- secure data sharing and dissemination (internally and externally) and
- applys Image and Signal based intelligence (IMINT and SIGINT).



Kristoffer Martin

55/Male
Sweden

Kristoffer is a government official in Stockholm, who is responsible for the analysis, elaboration and preparation of security concepts at the country level.

As a policy maker, it is his job to identify vulnerabilities in national security and support the armed forces with modern solutions.

KRISTOFFER HAS THE FOLLOWING LIMITATIONS

Even though a lot of threats are spread through online media, Kristoffer is not able to search the world wide web for potential threats on his own.

More training is required to educate employees on online safety.

Multiple pieces of software are used at once, which often generates certain limitations during the exchange of information.

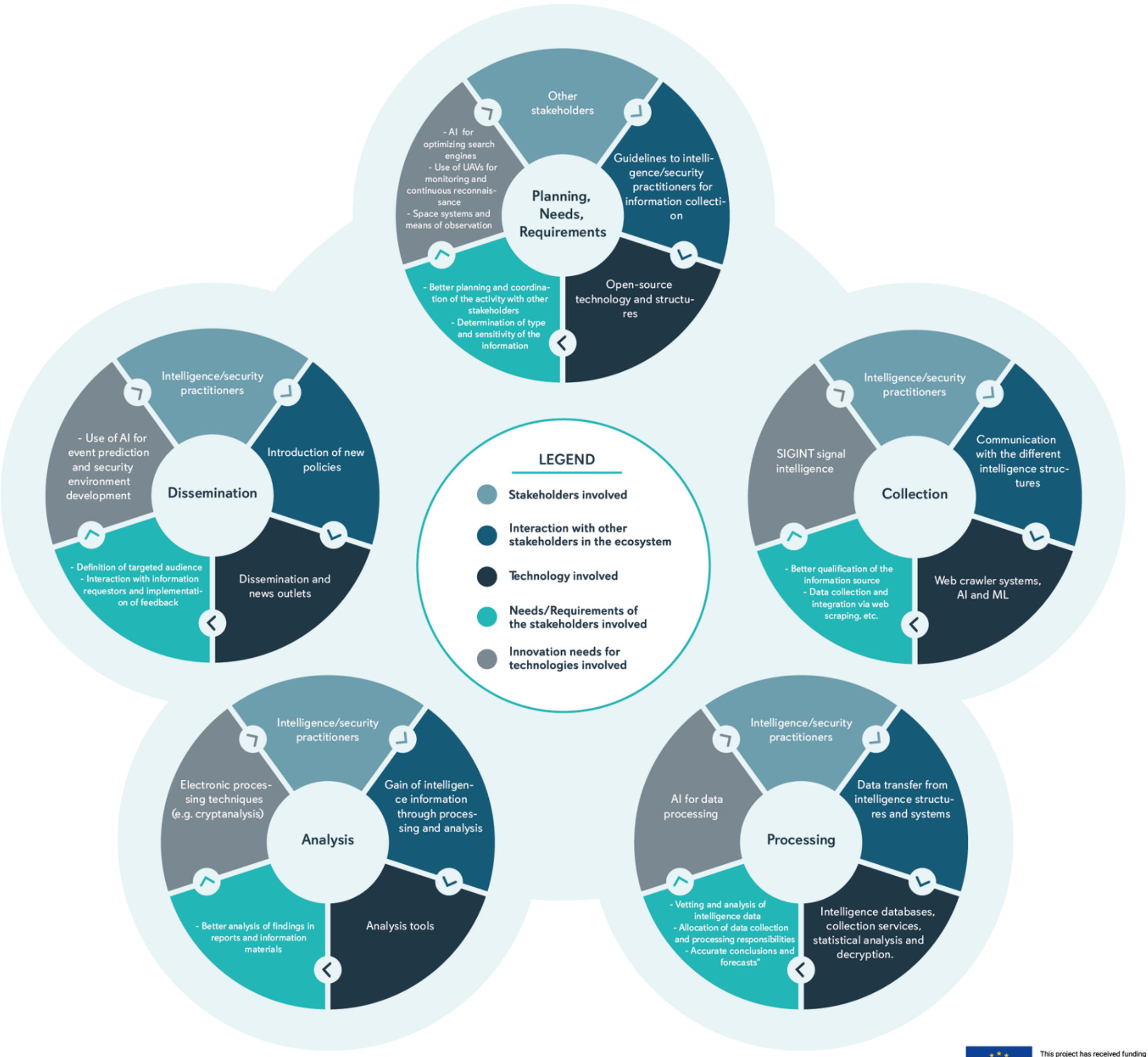
KRISTOFFER IS LOOKING FOR A SOLUTION TO

- counter potential terrorist threats via social media,
- increase communication with the intelligence services for better identification of potential threats and
- communicate the needs of his government to the security practitioners.

KRISTOFFER IS USING A SOLUTIONS FOR

- data enrichment from external databases and
- decision management.

NOTIONES INTELLIGENCE CYCLE



Planning, Needs, Requirements

Other stakeholders

Guidelines to intelligence/security practitioners for information collection

Open-source technology and structures

- Better planning and coordination of the activity with other stakeholders
- Determination of type and sensitivity of the information

- AI for optimizing search engines
- Use of UAVs for monitoring and continuous reconnaissance
- Space systems and means of observation

Collection

Intelligence/security practitioners

Communication with the different intelligence structures

Web crawler systems, AI and ML

- Better qualification of the information source
- Data collection and integration via web scraping, etc.

SIGINT signal intelligence

Processing

Intelligence/security practitioners

Data transfer from intelligence structures and systems

Intelligence databases, collection services, statistical analysis and decryption.

- Vetting and analysis of intelligence data
- Allocation of data collection and processing responsibilities
- Accurate conclusions and forecasts"

AI for data processing

Analysis

Intelligence/security practitioners

Gain of intelligence information through processing and analysis

Analysis tools

- Better analysis of findings in reports and information materials

Electronic processing techniques (e.g. cryptanalysis)

Dissemination

Intelligence/security practitioners

Introduction of new policies

Dissemination and news outlets

- Definition of targeted audience
- Interaction with information requestors and implementation of feedback

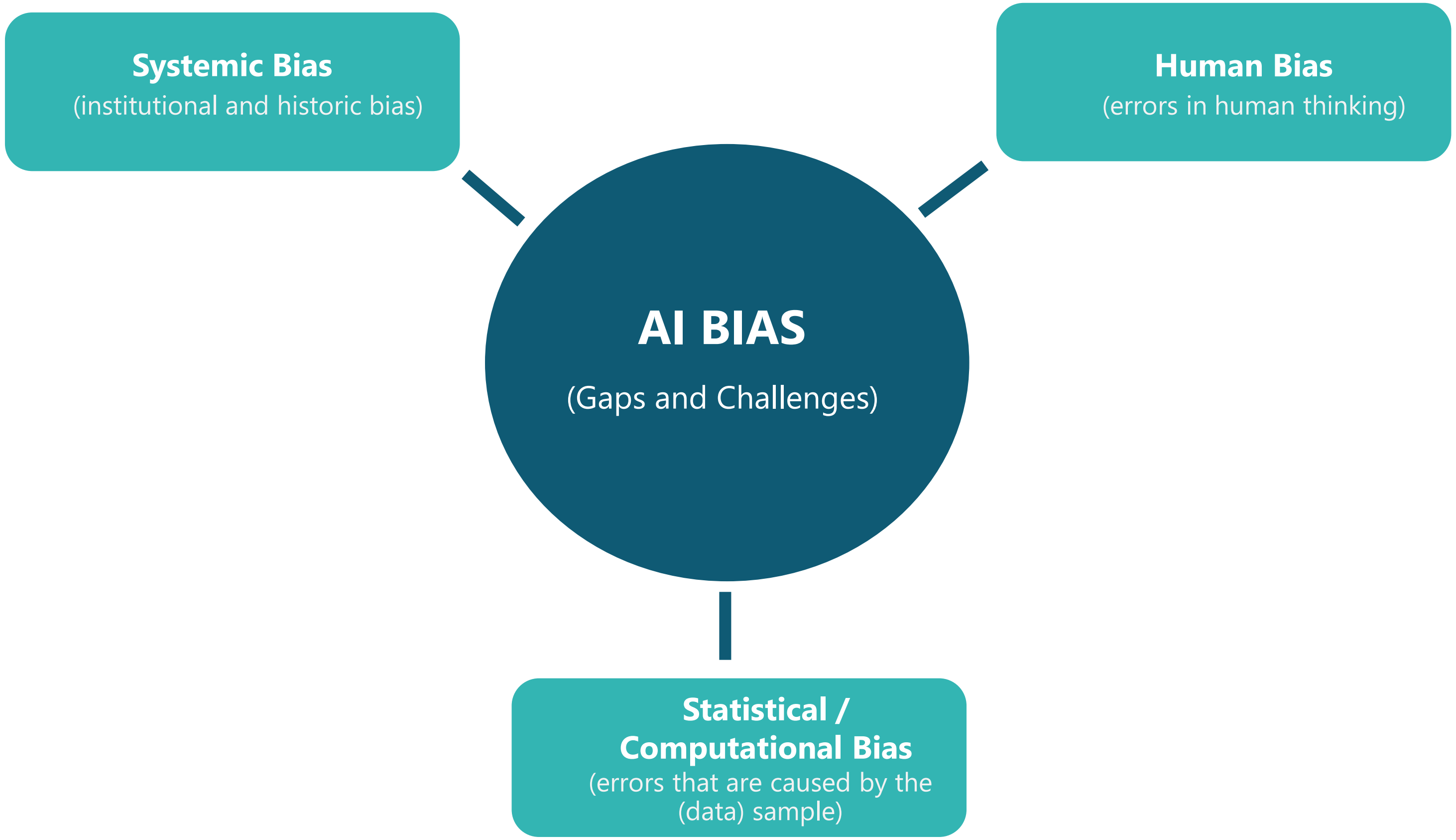
- Use of AI for event prediction and security environment development

LEGEND

- ● Stakeholders involved
- ● Interaction with other stakeholders in the ecosystem
- ● Technology involved
- ● Needs/Requirements of the stakeholders involved
- ● Innovation needs for technologies involved

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.

AI BIAS IN LEAs DECISION MAKING



AI BIAS

(Gaps and Challenges)

Systemic Bias
(institutional and historic bias)

Human Bias
(errors in human thinking)

Statistical / Computational Bias
(errors that are caused by the (data) sample)

Thank you for your attention!
Contact us, get involved, stay updated:

✉ office@notiones.eu

🌐 www.notiones.eu

@NOTIONES_EU

in NOTIONES

popAI project

Dr Dimitris M. Kyriazanos
Project Coordinator, NCSR Demokritos, Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

popAI project

Dr Dimitris M. Kyriazanos, Project Coordinator

NCSR Demokritos

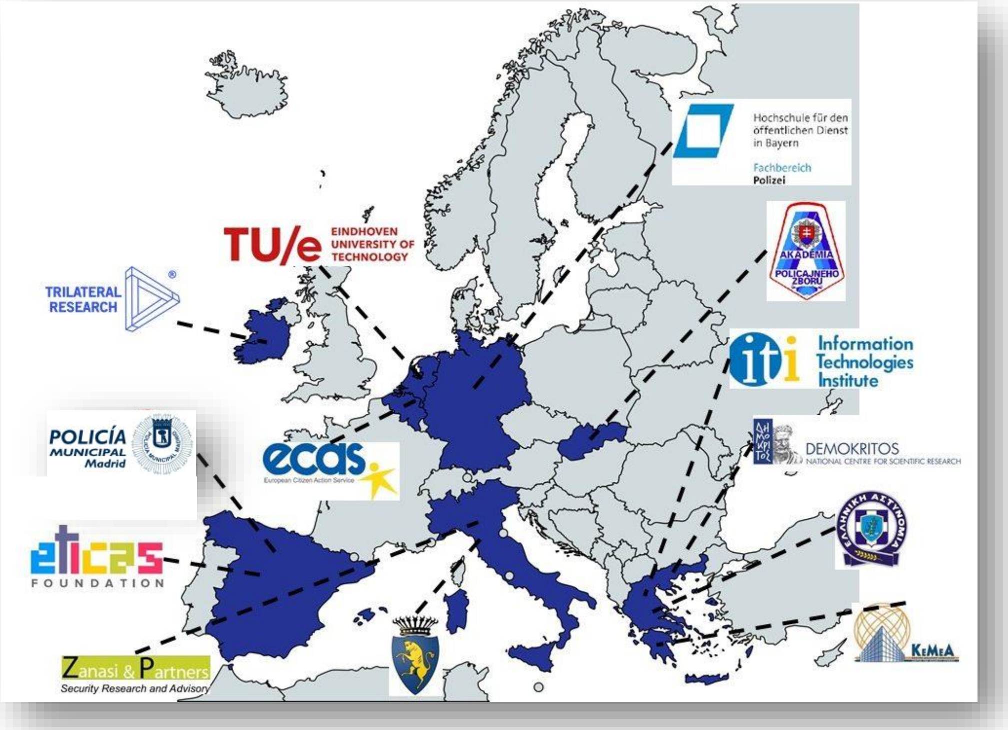
Email: dkyri@iit.demokritos.gr

Office: +30 2106503150

popAI is funded by the Horizon 2020 Framework Programme of the European Union for Research and Innovation. GA number: 101022001

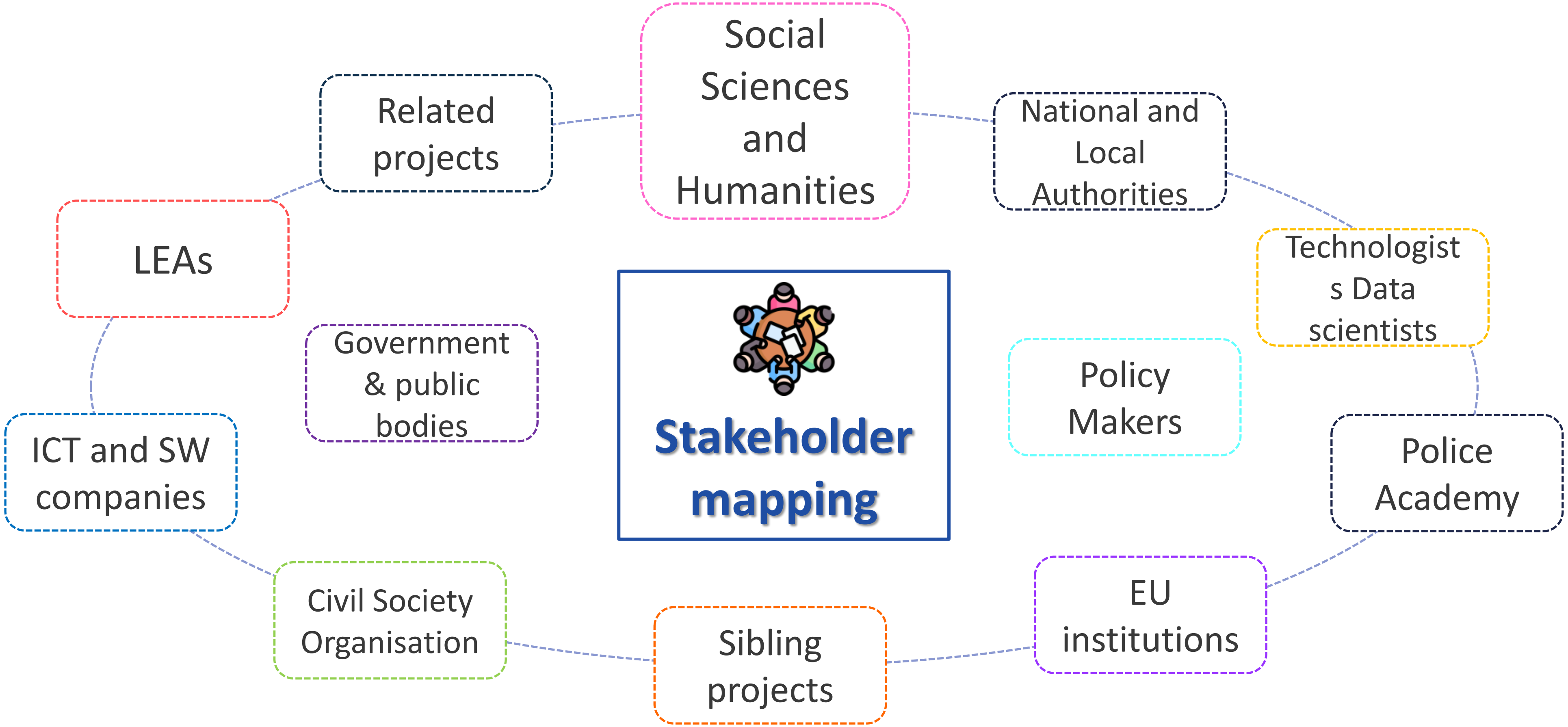
popAI – in a nutshell

Main objective	Main results
pop AI is a **24 month Coordination and Support Action**, bringing together security practitioners, AI scientists, ethics and privacy researchers, civil society organisations as well as social Sciences and humanities experts ..aiming to **boost trust** in AI **by increasing awareness** and current **social engagement**, consolidating distinct spheres of knowledge, and delivering a unified European view and recommendations, creating an ecosystem and the structural basis for **a sustainable and inclusive European AI hub for LEA** **SU-AI Cluster**	**popAI Methodology:** **Analysis of theoretical** legal, ethical, social and technical framework related to the use of AI tools in the security domain **Empirical Research** on the AI tools in the security domain, raising awareness, societal acceptance and ethics engaging **an inclusive EU AI ecosystem** **Leading to results:** **Pandect of recommendations** for the ethical use of AI for Law Enforcement Authorities (LEAs) **A practical ethics toolbox for assessing use of AI in Civil Security** and **holistic AI taxonomy** including functionalities, controversies and social acceptance, organisational and legal aspects


Hochschule für den öffentlichen Dienst in Bayern
Fachbereich Polizei
TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY
TRILATERAL RESEARCH
AKADEMIA POLICAJNÉHO ZBORU
Information Technologies Institute
POLICÍA MUNICIPAL Madrid
ecas
European Citizen Action Service
DEMOKRITOS NATIONAL CENTRE FOR SCIENTIFIC RESEARCH
eticas FOUNDATION
Zanasi & Partners
Security Research and Advisory
KEMEA

https://www.pop-ai.eu/

popAI – Ecosystem & Stakeholders


Stakeholder mapping
Social Sciences and Humanities
Related projects
National and Local Authorities
LEAs
Technologists Data scientists
Government & public bodies
Policy Makers
ICT and SW companies
Police Academy
Civil Society Organisation
Sibling projects
EU institutions

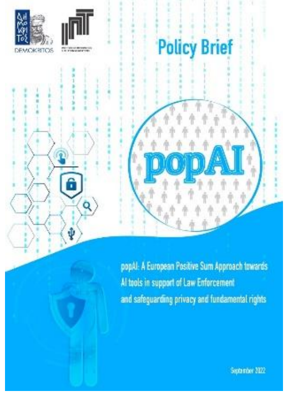
https://www.pop-ai.eu/

popAI project

Introduction

popAI Highlights

1st Year Policy Brief

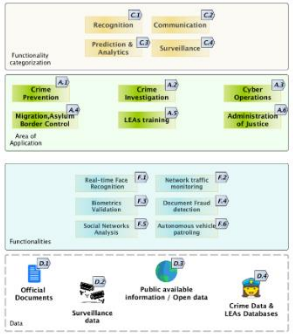


Policy Brief

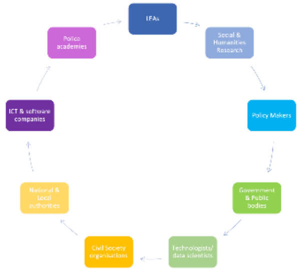
popAI: A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

September 2022

Systemising Knowledge for AI in Civil Security: functionalities and legal taxonomies


C.1 Recognition
C.2 Communication
C.3 Prediction & Analytics
C.4 Surveillance
Functionality categorization
A.1 Crime Prevention
A.2 Crime Investigation
A.3 Cyber Operations
A.4 Migration,Asylum Border Control
A.5 LEAs training
A.6 Administration of Justice
Area of Application
F.1 Real-time Face Recognition
F.2 Network traffic monitoring
F.3 Biometrics Validation
F.4 Document Fraud detection
F.5 Social Networks Analysis
F.6 Autonomous vehicle patroling
Functionalities
D.1 Official Documents
D.2 Surveillance data
D.3 Public available information / Open data
D.4 Crime Data & LEAs Databases
Data

The Map of AI in policing innovation ecosystem and stakeholders


LEAs
Social & Humanities Research
Policy Makers
Government & Public bodies
Technologists/ data scientists
Civil Society organisations
National & Local authorities
ICT & software companies
Police academies

Listening to & Discussing with Society

popAI

European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

What do you think about the use of Artificial Intelligence to prevent Crime, enhance Security, assist in Law Enforcement and Justice?

Fill in the anonymous questionnaire here: https://crowdsourcing.ecas.org/en/popai

Ecosystem engagement: SU-AI clustering & joint activities plan

popAI

ALIGNER

STARLIGHT

Connecting with more than 15 relevant projects, EU bodies and initiatives

Ecosystem engagement:

Conducted 5 Policy Labs

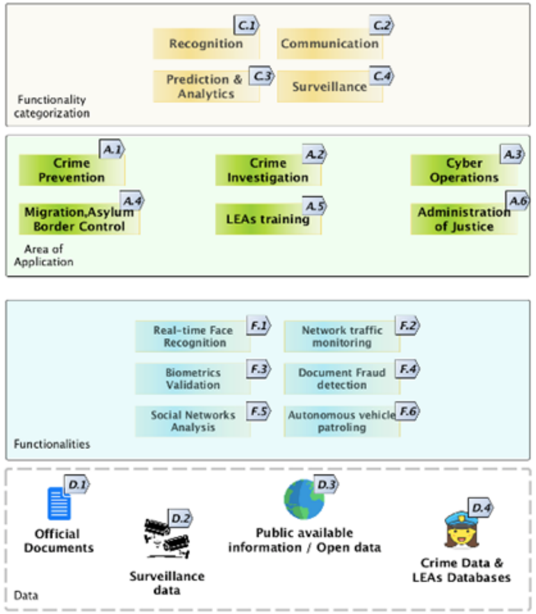
https://www.pop-ai.eu/policy_labs/

popAI Taxonomy

We have created a series of taxonomies that organise the knowledge around AI, its legal, ethical and social concerns:

- A Functionality taxonomy
- A Legal taxonomy
- An Ethical taxonomy

Systemising Knowledge for AI in Civil Security



Functionality categorization

C.1 Recognition

C.2 Communication

C.3 Prediction & Analytics

C.4 Surveillance

Area of Application

A.1 Crime Prevention

A.2 Crime Investigation

A.3 Cyber Operations

A.4 Migration,Asylum Border Control

A.5 LEAs training

A.6 Administration of Justice

Functionalities

F.1 Real-time Face Recognition

F.2 Network traffic monitoring

F.3 Biometrics Validation

F.4 Document Fraud detection

F.5 Social Networks Analysis

F.6 Autonomous vehicle patroling

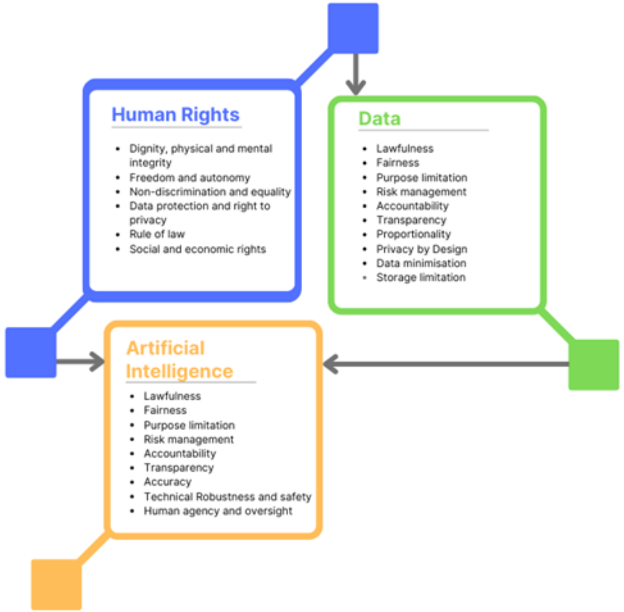
Data

D.1 Official Documents

D.2 Surveillance data

D.3 Public available information / Open data

D.4 Crime Data & LEAs Databases



Human Rights

- Dignity, physical and mental integrity
- Freedom and autonomy
- Non-discrimination and equality
- Data protection and right to privacy
- Rule of law
- Social and economic rights

Data

- Lawfulness
- Fairness
- Purpose limitation
- Risk management
- Accountability
- Transparency
- Proportionality
- Privacy by Design
- Data minimisation
- Storage limitation

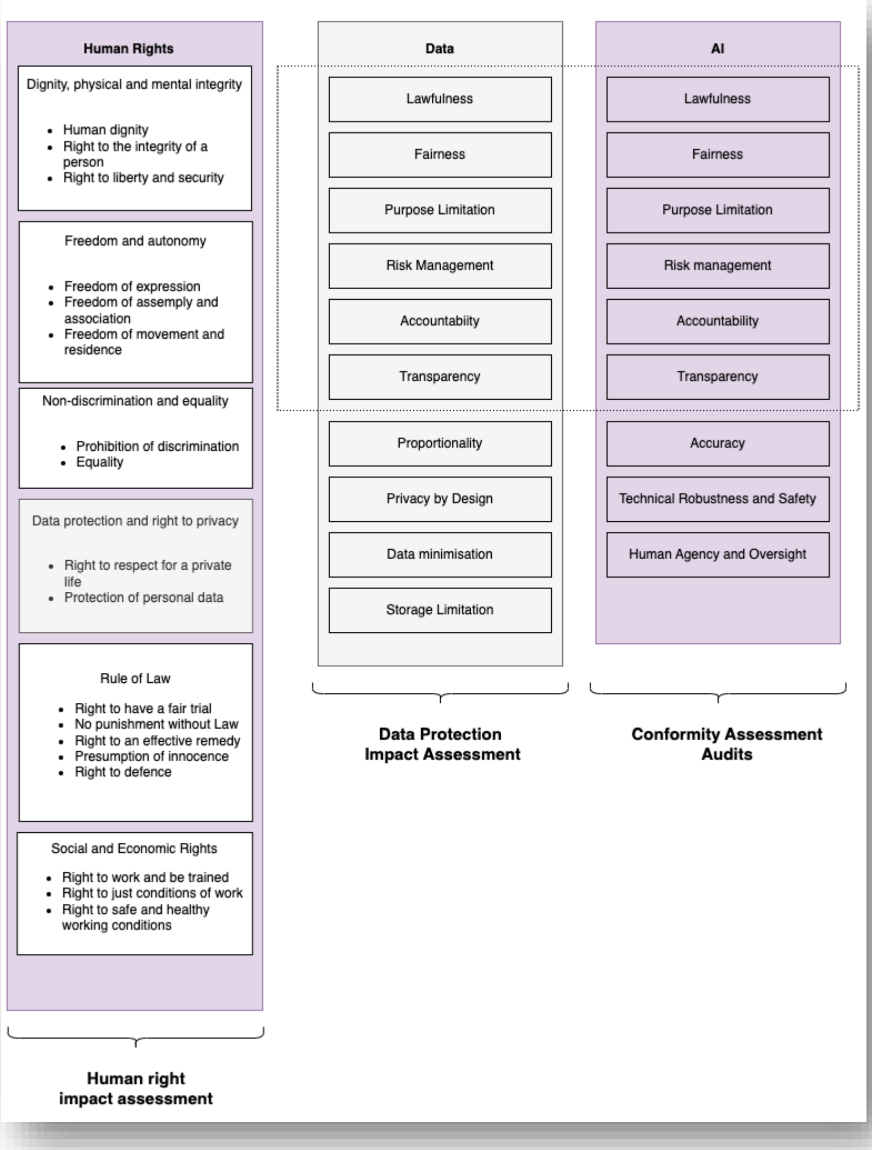
Artificial Intelligence

- Lawfulness
- Fairness
- Purpose limitation
- Risk management
- Accountability
- Transparency
- Accuracy
- Technical Robustness and safety
- Human agency and oversight

Legal Taxonomy

This classification aims to simplify the categorization of regulations that apply to AI in order to enable to

1) better compare how regulations address social concerns,
2) identify areas and intersection of areas that are currently not covered by binding and non-binding instruments and
3) promote a unified approach that merges human rights, data and AI-related concerns.



Human Rights

Dignity, physical and mental integrity

- Human dignity
- Right to the integrity of a person
- Right to liberty and security

Freedom and autonomy

- Freedom of expression
- Freedom of assembly and association
- Freedom of movement and residence

Non-discrimination and equality

- Prohibition of discrimination
- Equality

Data protection and right to privacy

- Right to respect for a private life
- Protection of personal data

Rule of Law

- Right to have a fair trial
- No punishment without Law
- Right to an effective remedy
- Presumption of innocence
- Right to defence

Social and Economic Rights

- Right to work and be trained
- Right to just conditions of work
- Right to safe and healthy working conditions

Human right impact assessment

Data

Lawfulness

Fairness

Purpose Limitation

Risk Management

Accountabiity

Transparency

Proportionality

Privacy by Design

Data minimisation

Storage Limitation

Data Protection Impact Assessment

AI

Lawfulness

Fairness

Purpose Limitation

Risk management

Accountability

Transparency

Accuracy

Technical Robustness and Safety

Human Agency and Oversight

Conformity Assessment Audits

Ethics Toolbox

popAI is creating an Ethics toolbox to help LEAs navigate the world of Responsible AI.

The ethics toolbox includes:

- An open-access interactive page that will use the legal, ethical and functionality taxonomy we have created to allow people to easily search legal, social and ethical aspects of AI applications in security
- 8 educational videos that will answer the questions that we collected from LEAs on Responsible AI
- A glossary

popAI – Let’s stay connected

Visit our website: www.pop-ai.eu

@popaiproject

/company/popai-project/

popAI is funded by the Horizon 2020
Framework Programme of the European Union
for Research and Innovation. GA number: 101022001

popAI Final Conference

Brussels, Belgium

September 2023

https://www.pop-ai.eu/

popAI

Thank you

ΔΗΜΟΚΡΙΤΟΣ
DEMOKRITOS
NATIONAL CENTRE FOR SCIENTIFIC RESEARCH

TRILATERAL RESEARCH

eticas
FOUNDATION

KEMEA

iti Information Technologies Institute

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Zanasi & Partners
Security Research and Advisory

ecas
European Citizen Action Service

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

Hochschule für den
öffentlichen Dienst
in Bayern

Fachbereich
Polizei

POLICÍA
MUNICIPAL
Madrid

POLICÍA MUNICIPAL MADRID

AKADÉMIA
POLICAJNÉHO
ZBORU

https://www.pop-ai.eu/ popAI

Questions & Answers

popAI project

Greek policy lab

Anthoula Bania

Hellenic Police, Greece

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

1st Stakeholder Policy Lab
Greece

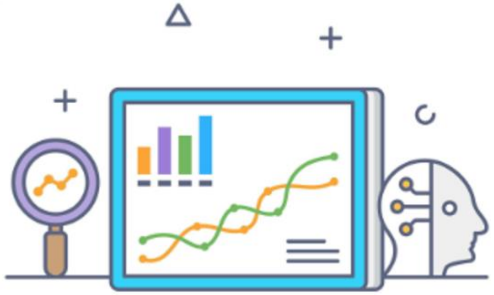
25th May 2022

(online meeting)

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

Case Studies

1. Predictive, research, and detection systems using crime data to improve policing and combat crime



2. Systems for predicting dangerous driving using video footage from traffic management cameras or other real-time footage to prevent traffic accidents.

Methodology

1. Online meeting: more than 25 persons attending
   - Hellenic Police representative (*operational* approach)
   - IT companies (*technical* approach)
2. Open discussion: 3 groups (from different disciplines) in 3 break-out sessions
3. The moderator illustrated the key outcomes in the plenary meeting
4. Second open discussion: 3 groups (from different disciplines) in 3 break-out sessions
5. Definition of recommendations to overcome the emerged challenges.

1st Case Study

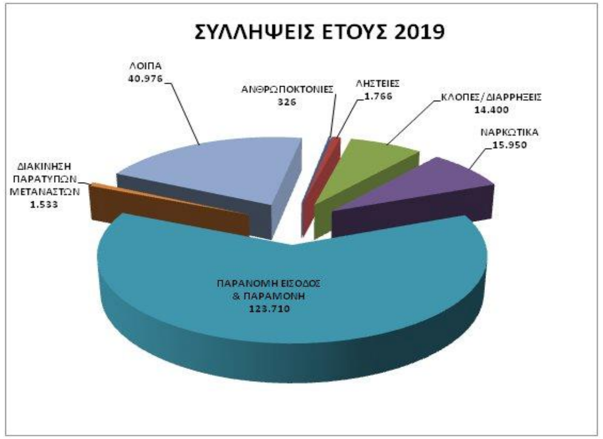
Predictive, research, and detection systems using crime data to improve policing and combat crime

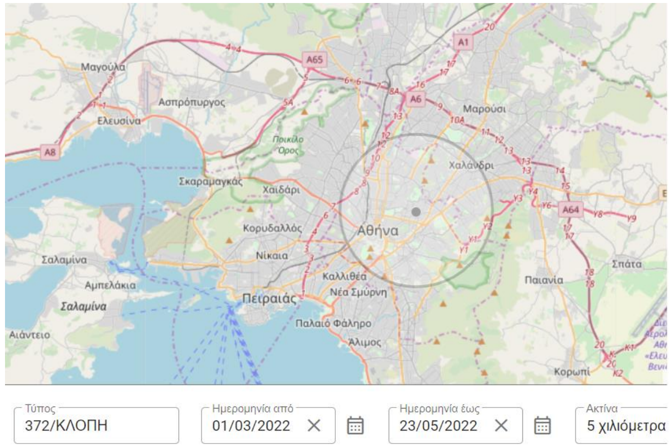
Important! Explaining and clarifying key concepts of the discussion when there are groups from different disciplines

- Descriptive analytics: what has already happened
- Predictive analytics: what will happen
- Prescriptive analytics: what should happen

popAI Policy Labs

1st Policy Lab - Greece





Τύπος: 372/ΚΛΟΠΗ

Ημερομηνία από: 01/03/2022

Ημερομηνία έως: 23/05/2022

Ακτίνα: 5 χιλιόμετρα

1st Case Study

AS IS

- ✓ Application-system in which all offences and incidents of police interest are reported and captured in real time.
- ✓ No use of AI
- ✓ Publish statistics of the main forms of crime
- ✓ Specific actions, which aim to provide immediate response

1st Case Study - Concerns - questions

- ✓ Where will my resources be spent the next day?
- ✓ How will I make effective use of staff?

Use of AI at technical and operational levels:

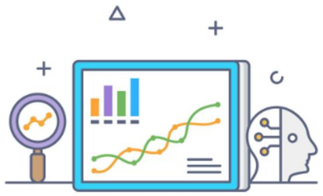
- ✓ ensuring proper planning;
- ✓ accuracy and reliability;
- ✓ transparency;
- ✓ safe and correct use of the system;
- ✓ capability of upgrading/reconfiguration.

1st Case Study - Potential benefits

- ✓ Appropriate and targeted allocation and distribution of resources minimizing potential human biases
- ✓ Not easily processed manually
- ✓ advise/support decision-making on different levels of policing

1st Case Study - Potential challenges

- ✓ Risk of impartial control and bias of the system
  - → Negative feedback loop
- ✓ Overreliance on the system



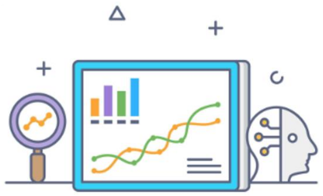
1st Case Study - Recommendations

Organizational/Regulation Level

- ✓ **Support** the decision making **not to make** the decisions
- ✓ **Certification** of system accountability

Technical Level

- ✓ Systems need to be constantly improved/ updated
- ✓ Transparency: **open-source** algorithms



2st Case Study

Systems for predicting dangerous driving using video footage from traffic management cameras or other real-time footage to prevent traffic accidents

Initial assessment

✓ Prevention of traffic accidents

✓ Ethical dimensions of a potentially emerging mass surveillance system

2st Case Study - Potential benefits

✓ Train algorithms in scoring driving behaviour as low, medium, and high risk

✓ Interoperability - inform the respective governmental bodies

2st Case Study - Potential challenges

✓ Risk of abusing sensitive personal data

✓ Potential abuse of the system as third parties

2st Case Study - Recommendations

Organizational/Regulation Level

- ✓ Open data
- ✓ Operators’ training

Technical Level

- ✓ Securing user access
- ✓ Data security – system

popAI project

German policy lab

Pinelopi Troullinou

Trilateral Research, Ireland

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

2nd Stakeholder Policy Lab Germany

15th September 2022

(online meeting)

Hochschule für den öffentlichen Dienst in Bayern

Fachbereich **Polizei**

Case Studies

1. AI as a support in mission control

2. AI as support for the processing of material of sexual exploitation of children (CSAM) and its evaluation

Methodology

1. Interactive workshop (2 hours)
2. 13 online participants with the following backgrounds:
   - LEAs
   - Technical experts
   - Legal and ethics experts
3. Discussions on the 2 case studies and wrap-up session

1st case study

AI as support in mission control

Operational command initial situation

Factors	Description
Emergency Call	An emergency call is received at the operations centre. Apparently there was a dispute between two neighbours. One person was injured by a knife.
Situation at the Operations Centre	The officer-in-charge checks the control centre to see which patrols are in the area. There are three possible patrols: • Patrol 1: 1km away, patrolmen on duty since 8h, no special training of patrol officers, no special equipment carried along • Patrol 2: 2km away, Patrol officers on duty since 4h, no special training for patrolmen, Taser is carried. • Patrol 2: 3km away, patrol officers on duty for 2h, one negotiation-trained officer in the car. • no special equipment is carried along
Decision at the Operations Centre	The officer-in-charge sends patrols 2 and 3 to the scene. Meanwhile, patrol 1 covers patrol areas 1, 2 and 3.

1st case study

AI as support in mission control

Problems

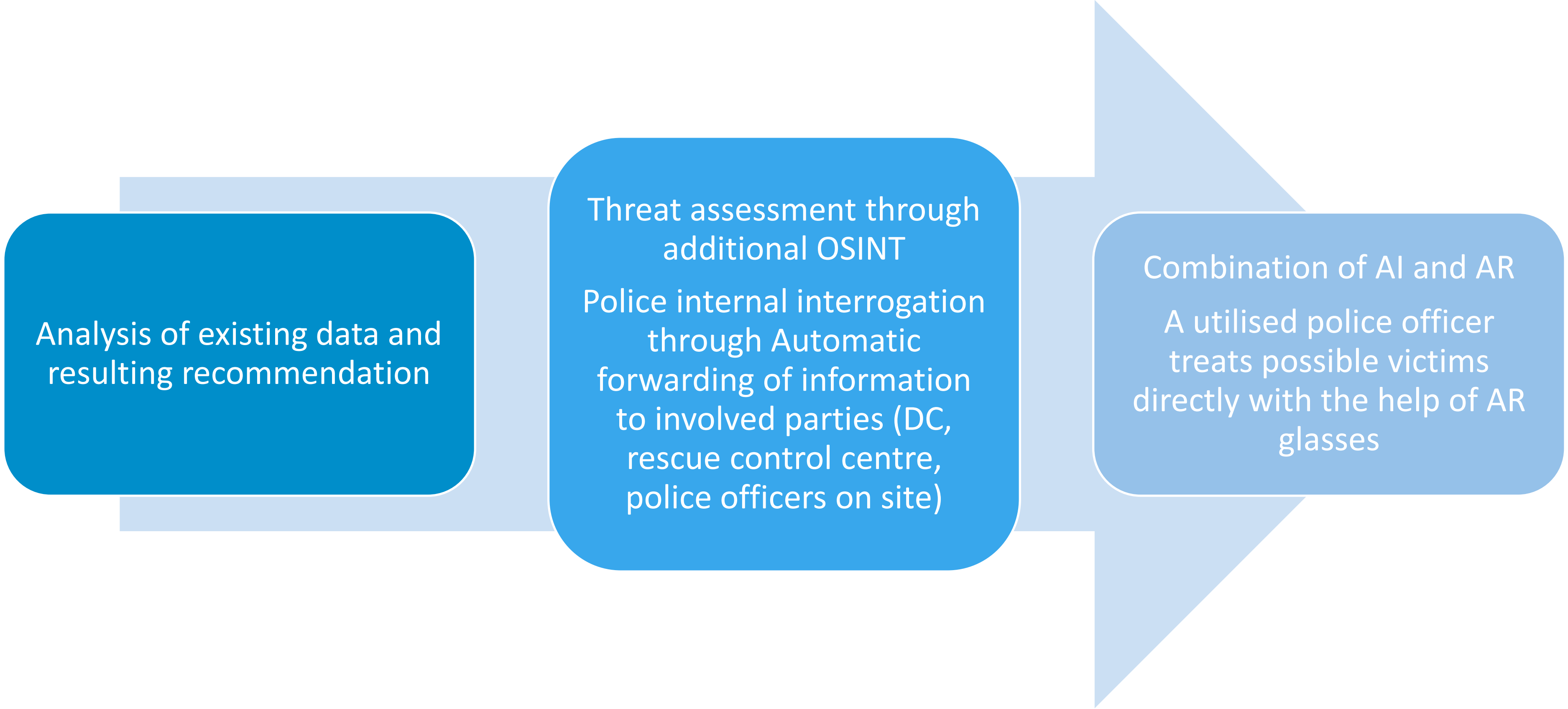
Facorts	Description
Use of the available data	• Command must make a decision in a reasonable amount of time • Obtaining data on the different strips takes time • Decision is made without knowledge of the entire data situation
Role of the Operations Manager	• Personal experience has an influence on decision-making • Mission control and person in charge can change at very short notice

Higher susceptibility to errors
due to the human factor

1st case study

AI as support in mission control

Use of AI



Analysis of existing data and resulting recommendation

Threat assessment through additional OSINT

Police internal interrogation through Automatic forwarding of information to involved parties (DC, rescue control centre, police officers on site)

Combination of AI and AR

A utilised police officer treats possible victims directly with the help of AR glasses

2nd case study

AI as support for the processing of material of sexual exploitation of children (CSAM) and its evaluation

Operational initial situation

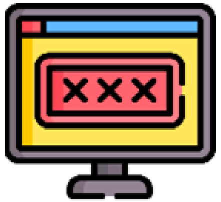
Factors	Description
Seized material	Various hard disks and data carriers are seized from one suspect
Incoming Suspicious Activity Reports	Within the framework of international police reporting systems, hundreds of suspicious online contents are reported to the German police every day.
Visual inspection	All suspicious and seized material is individually visually inspected manually by the officers

2nd case study

AI as support for the processing of material of sexual exploitation of children (CSAM) and its evaluation

Problems

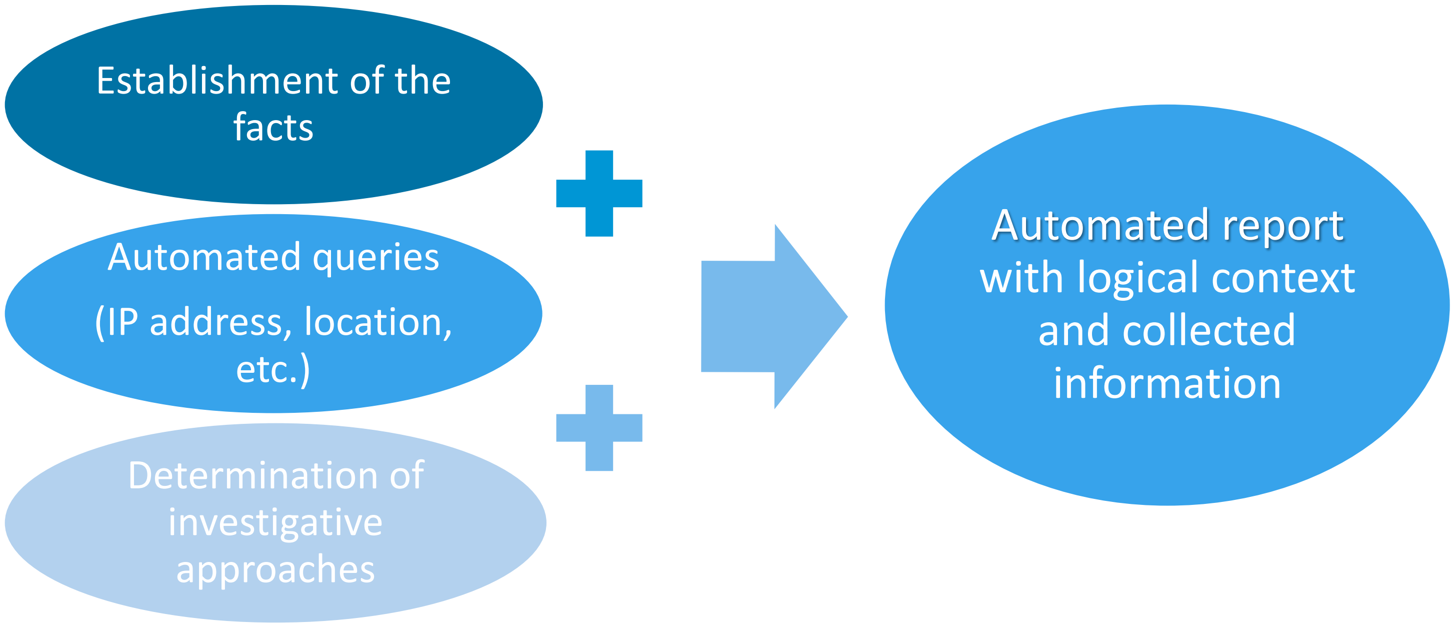
Factors	Description
Visual evaluation	• Investigative approaches can only be created to a limited extent with the human eye • Psychologically stressful • Time-intensive
Administrative effort	• A report must be prepared for each case



2nd case study

AI as support for the processing of material of sexual exploitation of children (CSAM) and its evaluation

Application of AI



Establishment of the facts

+

Automated queries

(IP address, location, etc.)

+

Determination of investigative approaches

Automated report with logical context and collected information

2nd case study

AI as support for the processing of material of sexual exploitation of children (CSAM) and its evaluation

Key findings

- AI support in mission control is rather **practical in urban areas** than in rural areas
- LEAs see AI application rather in **scenario 2** than in scenario 1
- Discussed scenarios are **technically feasible but ethical and legal hurdles** might exist
- No black box approach! **Traceability** of decisions of the AI is crucial
- **No significant risk of bias** as the amount of training material is so high and various that the risk for a bias is estimated as low

popAI project
Slovak policy lab

Mojmír Mamojka
Academy of the Police Force in Bratislava, Slovakia

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

3rd Stakeholder Policy Lab
Slovakia
13th December 2022

(online meeting)

Case Study

AI tools in monitoring social networks

Methodology

1. Online and physical meeting
2. Participants from different sectors:
   - Academics (26)
     - Police Academy (25 – 14 of them were police officers)
     - Comenius University (1)
   - Tech designers (2) – Kempelen Institute of Intelligent Technologies
   - Policy Makers (7)
     - Institute of Administrative and Security Analysis of the Ministry of the Interior of the Slovak Republic
     - National Security Office Department of Education, Support and International Cooperation (1)
     - National Crime Agency (2)
     - Department of Computer Crime of the Presidium of the Police Force (3)
3. Open discussion and wrap up session

Case study

AI tools in monitoring social networks

Basic Legal Frame

European Data Protection Board
on the upcoming
Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence
(Artificial Intelligence Act)

Opinion of the
European Data Protection Supervisor

Case study

AI tools in monitoring social networks

Basic Legal Frame

Opinion of the

European Data Protection Supervisor

Point 27

The use of AI in the area of police and law enforcement requires ***area-specific, precise, foreseeable and proportionate <u>rules</u>*** *that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society.*

Case study

AI tools in monitoring social networks

Use of modern technologies in law enforcement in the Slovak Republic

in generalis

The National Search Information System,
which consists of several independent information systems.

Central Lustration Console
use software tools such as rsCASE computer programs, Analyst's Notebook, Autonomy IDOL Servere...

AFIS - Automated dactyloscopic identification system of persons
National database of DNA profiles and CODIS system - digitization of traces found at the crime scene and their subsequent comparison with databases

SOITRON
some police vehicles are equipped with technologies that enable the recognition of cars‘ license plates and their automatic lustration.

Case study

AI tools in monitoring social networks

Following the murder on Zámocká Street
in Bratislava, Slovakia

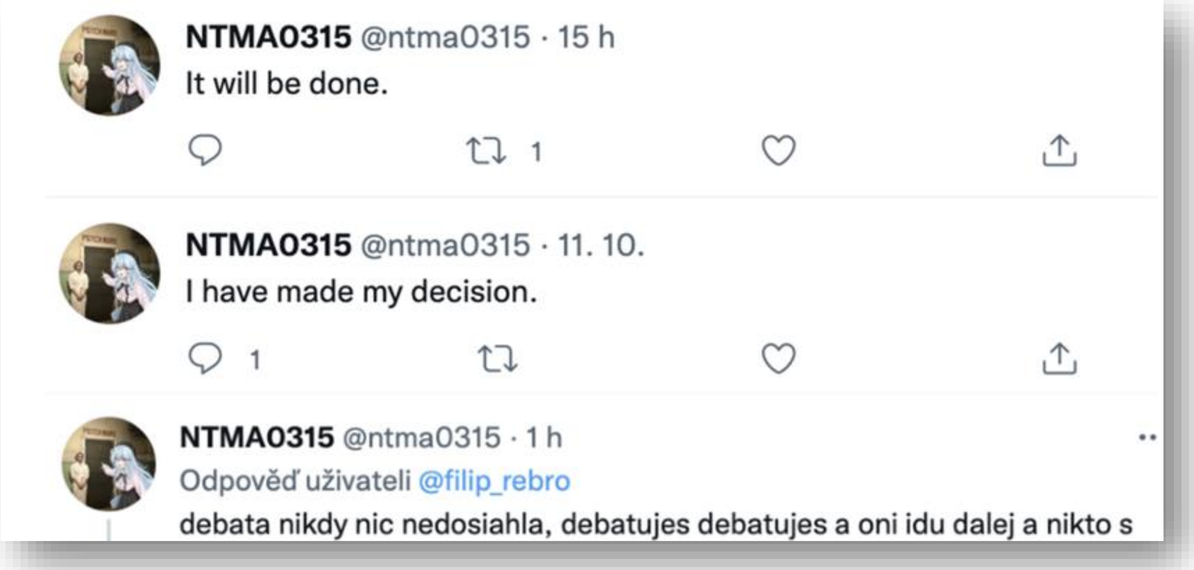
The perpetrator posted several hateful statuses against the LGBTI community
on an anonymous account only a few weeks before he murdered
2 people in front of the
,,Cafe Tepláreň" in Bratislava

Case study

AI tools in monitoring social networks

Evidence

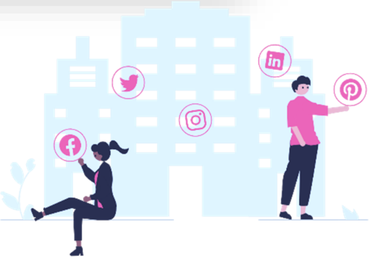
On the day of the murder, he posted a manifesto on the social network ...



NTMA0315 @ntma0315 · 15 h
It will be done.
1

NTMA0315 @ntma0315 · 11. 10.
I have made my decision.
1

NTMA0315 @ntma0315 · 1 h
Odpověď uživateli @filip_rebro
debata nikdy nic nedosiahla, debatujes debatujes a oni idu dalej a nikto s

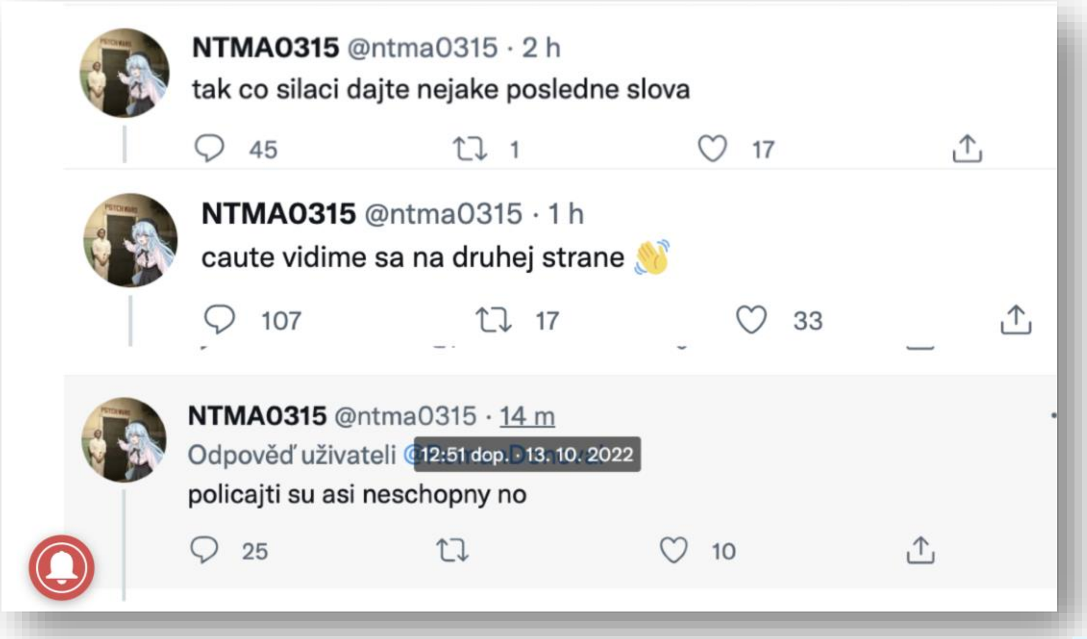


Case study

AI tools in monitoring social networks

Evidence

After the murder, he posted more tweets on the social network ...



NTMA0315 @ntma0315 · 2 h
tak co silaci dajte nejake posledne slova

NTMA0315 @ntma0315 · 1 h
caute vidime sa na druhej strane 👋

NTMA0315 @ntma0315 · 14 m
Odpověď uživateli @ 12:51 dop. 13. 10. 2022
policajti su asi neschopny no

Case study

AI tools in monitoring social networks

Key findings

The use of AI tools and the creation of relevant ethical standards is crucial

because <u>a large part of criminal activity</u>

<u>is moving from the "physical world" to the world of social networks.</u>

According to the available statistics, it may appear that the number of crimes committed in the Slovak Republic is decreasing, but one of the reasons is that the perpetrators of crimes that happen on the Internet are often anonymous and it is difficult or impossible to identify them.

Case study

AI tools in monitoring social networks

Key findings

Considering there is such a large amount of data on social networks and on the Internet in general it is **impossible** to monitor them without the help of AI tools.

However, **corresponding ethical standards must be created together with them** (among other things a proper balance between private law and public law in law enforcement),

which is why we appreciate the results of the popAI project so far.

Policy Labs

Final considerations

- The Stakeholder Policy Labs facilitate the exchange of knowledge, ideas and perspectives between LEAs and experts from different fields (academia, industry, policy-makers, etc.).
- This approach allows formulating new ideas for smart policies and testing the solutions to identified controversies in experimental models.
- Each policy lab addresses specific controversies and provides the local perspective of the analysed countries by bringing together relevant stakeholders from each region.
- The recommendations that emerged from the policy labs will be incorporated into the map of best practices emerging from popAI project and will form the basis of creating an ecosystem for a sustainable and inclusive social hub on the sound and ethical use of artificial intelligence by law enforcement agents (LEAs).

Questions & Answers

Round table discussion

15 min

ALLIES project

Denitsa Kozhuharova
Law and Internet Foundation, Bulgaria

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

ALLIES Project

The case of ethical AI in LEAs decision-making

Say ‘Hi’ to ALLIES

The aim of ALLIES is to support micro (and small) Hosting Service Providers (HSP) in complying with the requirements of the Terrorist Content Online Regulation (TCO) Regulation through the creation of the proper learning, training, experience sharing mechanisms as well as technical (AI) tools.

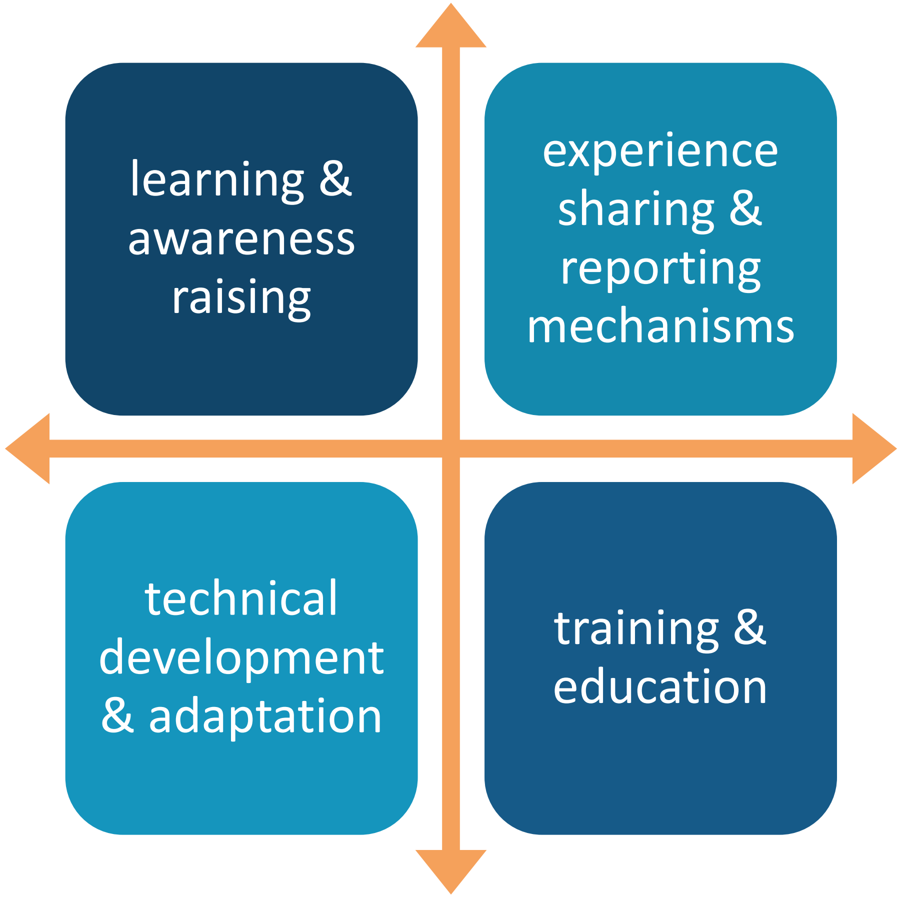
The ultimate outcomes that will derive from the project will include not only a higher number of TCO removed by micro (and small) HSPs, but also establishing a model of communication between such enterprises so that they share best practices and experiences with each other. Finally, the increase in the number of micro and small HSPs that will implement the TCO Regulation in a proper way is also a long-term outcome towards which ALLIES aims to work.

Consortium consists of 12 partners from 6 different EU Member States
– Bulgaria, Greece, Italy, Austria, Spain, Cyprus.

The project is built on four main pillars

Overview of the project

Complementing and cooperating with each other, these four pillars will not only support HSPs, but will also contribute to the fulfilment of the TCO Regulation objectives.



learning & awareness raising

experience sharing & reporting mechanisms

technical development & adaptation

training & education

ALLIES Methodology & Approach

Prepare: The first months of the project are dedicated to conduct a well-rounded desktop and empirical research around the issues of online radicalisation, extremism and terrorism, capitalising on existing knowledge as well as on the expertise stemming from the consortium end-users alignment with their networks. This should result in the development of a **unified taxonomy for online terrorist behaviours enablers, motives, and incentives**. The data collection will consider their operational but also **training needs** to allow the crafting of a **bespoke curricula**. The scope of the end-users' needs' assessment will unfold in the partner countries to allow their unique perspectives to be forefront, considering the local legal, technical but also cultural particularities. The outputs of this analysis will feed to the **awareness raising, training and education** pillar of ALLIES project, being simultaneously reviewed and updated from the inputs derived from the terrorist related data acquisition and AI content analysis.

Develop: Following the preparation phase of the project, two development iterations have been foreseen during ALLIES's lifespan: (a) **initial design and development phase** (prototyping), and (b) **continuation of the development** along with the **integration** of the tools. The initial phase will capitalise on the findings from previous activities, while the final phase will introduce the feedback received from the first pilot demonstration of the ALLIES solutions. The final tools (Semi-automated AI tool suite and Training platform) will be presented in the **final demo event**.

Timing

Prepare:

- Duration: M1-M4

Develop, Initial Design:

- Duration: M4-M14

Develop, Integration:

- Initiated at M7.
- Duration: M16-M21.
- First demo: M15.
- Final demo M24

ALLIES Methodology & Approach

Demonstrate: All the **tools** as well as the **training curricula** developed in the relevant WPs are going to be properly demonstrated in two pilots. The **first pilot phase** should function as a feedback and evaluation hub, where end users inside the consortium as well as invited HSPs through the elaborated stakeholder's network, will be able to provide their insights on the proposed solutions. During the **second pilot phase** the integrated solution are planned to be tested. The **final demonstration** of all the ALLIES tool suite, will be held in combination with the final ALLIES consortium meeting organised in a hybrid mode.

Propose: ALLIES final solution and relevant tools will be **duly communicated and disseminated** throughout the project's lifespan and beyond, proposing in that way to the end users (HSPs) one well-rounded solution for supporting them towards the **smooth implementation of the TCO Regulation**, also **increasing the volume of the removed TCO**, in full respect to fundamental rights.

Timing

Demonstrate:

- First Pilot Phase: M15
- Second Pilot Phase: M21-M23
- Final demo: M24

Develop, Initial Design:

- Duration: M4-M14

Develop, Integration:

- Initiated at M7.
- Duration: M16-M21.
- First demo: M15.
- Final demo M24

ALLIES Legal & Ethics Management

To properly manage ethical concerns and abide by legal requirements, LIF closely monitors all project activities and elaborates reports yearly on the potential risks and mitigation measures.

The following aspects fall in the scope of the **Legal & Ethics Management:**

- Project activities as such
- Use of ALLIES outputs by end users

Tools

- Internal training(s)
- Guidebook
- Uniform templates: informed consent, information policy, data sets assessments
- Data Management Plan
- Iterative meetings with the technical team

ALLIES Legal & Ethical Methodology & Approach

Following an end-user driven methodology, ALLIES aims to ensure the proper alignment of its outcomes with the operational and organisational needs of the final end-users, namely HSPs.

The Legal & Ethical Methodology will go beyond the project activities, to use best practices and established ethics standards when it comes to minimising algorithmic bias.

This will be achieved by:

- Use of robust and diverse data sets
- Having a diverse team of software developers
- Establishing a common understanding of the meaning of the Ethics Guidelines for Trustworthy AI in the project context.
- Design of tailored assessment mechanisms.

Questions & Answers

LAW-GAME project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Trusted Artificial Intelligence in Serious Games for Training LEAs

HOW AI HELPS LEAS TO BUILD AND OPERATE TRUSTED AI SYSTEMS

John Soldatos (jsoldat@innov-acts.com)

Scientific Advisor, INNOV-ACTS LIMITED

Innov-acts

01 **LAW-GAME Project Overview**

02 **Use of AI in LAW-GAME**

03 **AI for Predicting Indicators of Terroristic Attacks**

04 **Measures for Bias Alleviation & AI Act Compliance**

05 **How LAW-GAME helps LEAs with AI Bias**

LAW–GAME

Project Facts

- Full title: *An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions*
- Duration: 36 months, starting from 01.09.2021
- Budget: €7M
- Consortium: 19 partners from 11 European countries
- Demonstrations: in four European test sites
- Work Programme: Horizon 2020
- GA No: 101021714
- More Information: https://lawgame-project.eu/

Main Goal

The Main Goal of LAW-GAME project is to advance the capabilities of LEAs in:

1. **conducting forensic examination.**
2. **effective questioning, threatening, cajoling, persuasion, or negotiation**.
3. **recognizing and mitigating potential terrorist attacks.**

through a Novel VR-Based Gamification Framework approach.

LAW-GAME Critical Elements At a Glance

01

Complete Training System

Complete Gamified training system for LEAs

In-depth analysis of LEAs learning needs

Inspired by many disciplines .

02

LAW-GAME "Mini Games"

- ✓ Forensic Investigation
- ✓ Car Accident Analysis
- ✓ Police Interview
- ✓ Terroristic Attack Prevention

03

LAW-GAME Technological Pathways

Gamification
Virtual Reality
AI
Cloud Infrastructure

01 LAW-GAME Project Overview

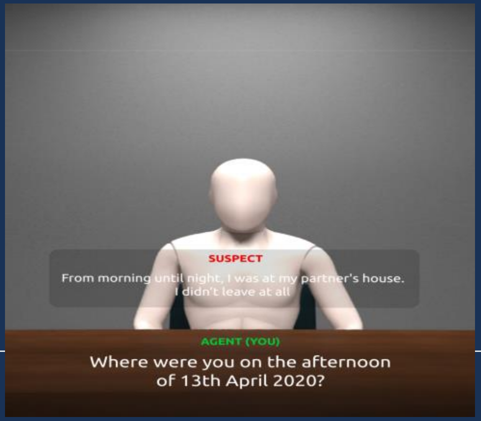
02 Use of AI in LAW-GAME

03 AI for Predicting Indicators of Terroristic Attacks

04 Measures for Bias Alleviation & AI Act Compliance

05 How LAW-GAME helps LEAs with AI Bias

The Different Uses of AI in LAW-GAME

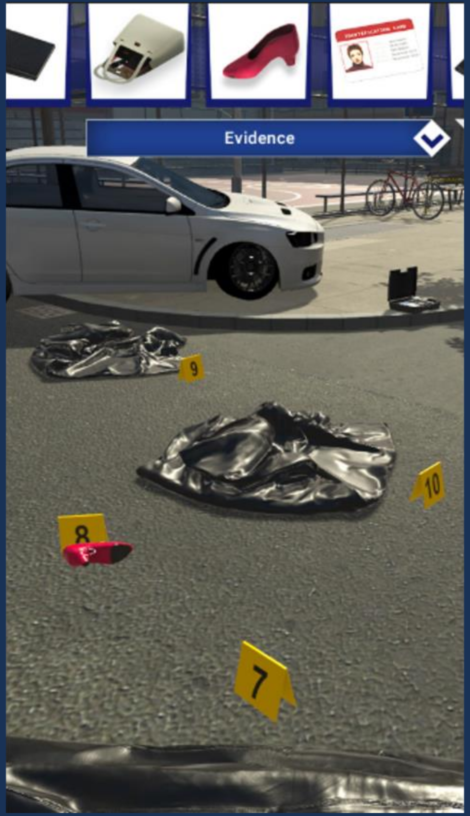

SUSPECT

From morning until night, I was at my partner's house. I didn't leave at all

AGENT (YOU)

Where were you on the afternoon of 13th April 2020?

1. Emotion and Stance Detection
2. AI Narration
3. AI-Based Semantic Analysis for Crime Scene Investigation
4. Visual Scene Analysis for Car Accidents
5. **AI based Prediction of Terroristic Indicators**



01 LAW-GAME Project Overview

02 Use of AI in LAW-GAME

03 AI for Predicting Indicators of Terroristic Attacks

04 Measures for Bias Alleviation & AI Act Compliance

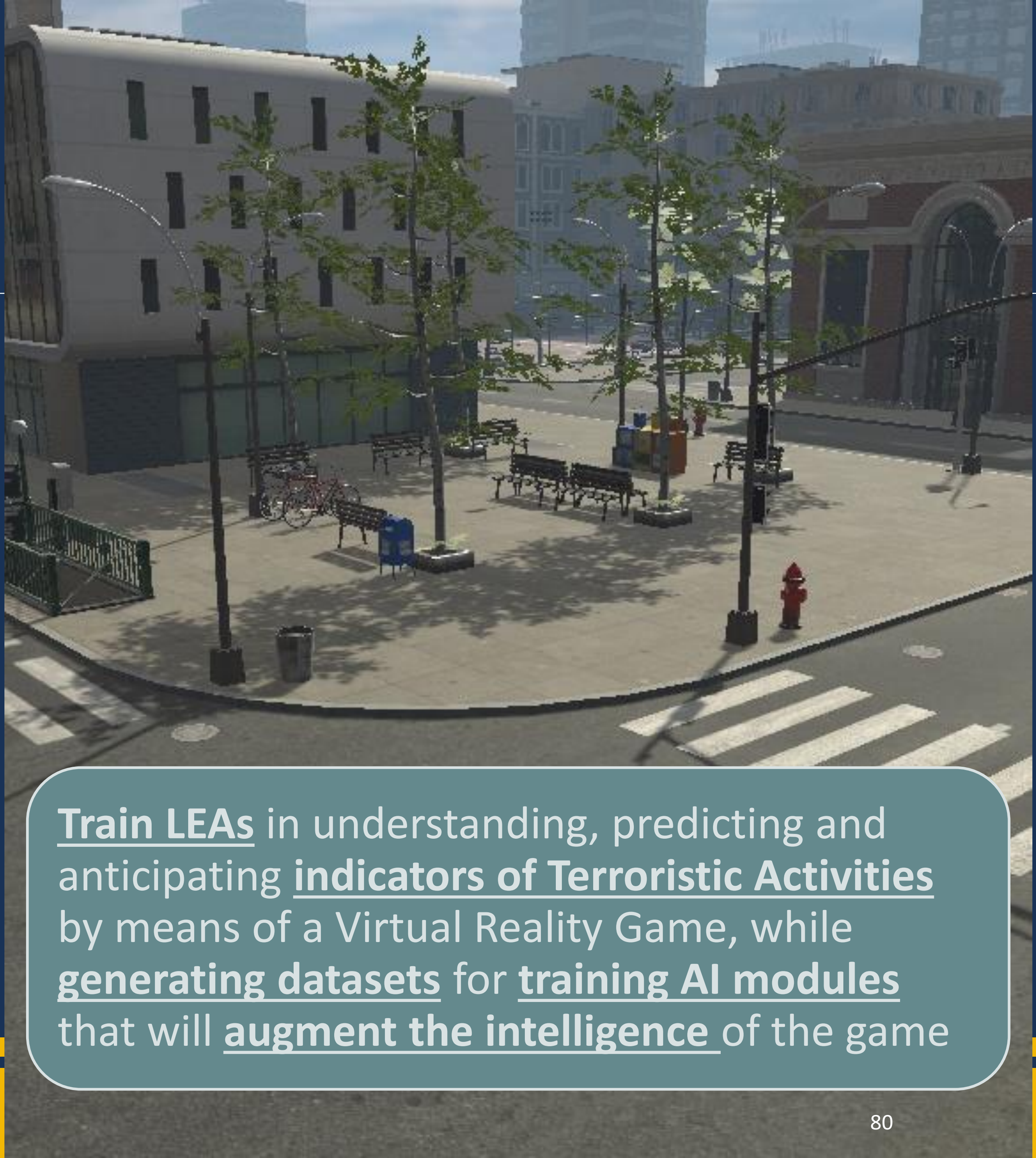
05 How LAW-GAME helps LEAs with AI Bias

Terrorist Attack Mini Game: Train Police Officers on Indicators of Terroristic Activities

Multi-player game, consisting of different groups of players;

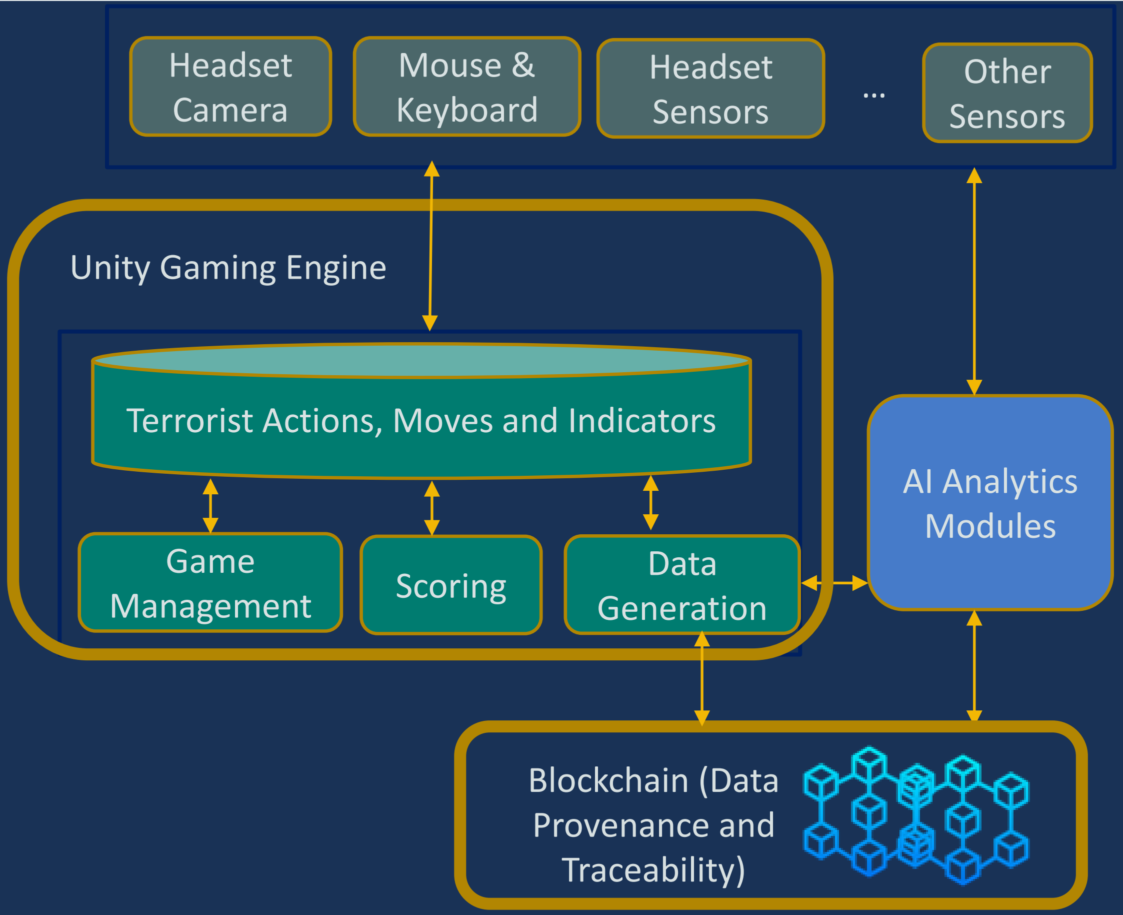
AI engine generates datasets of terrorist indicators and citizen movements;

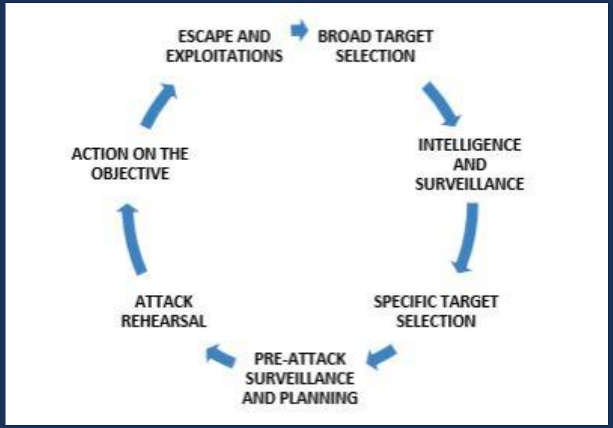
AI engine detects terrorist indicators.



Train LEAs in understanding, predicting and anticipating **indicators of Terroristic Activities** by means of a Virtual Reality Game, while **generating datasets** for **training AI modules** that will **augment the intelligence** of the game

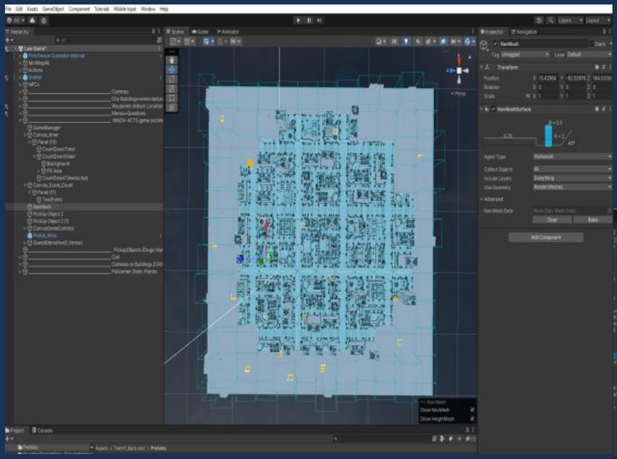
Simplified Architecture & Terroristic Modelling

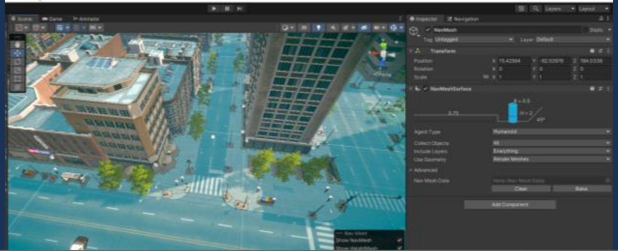


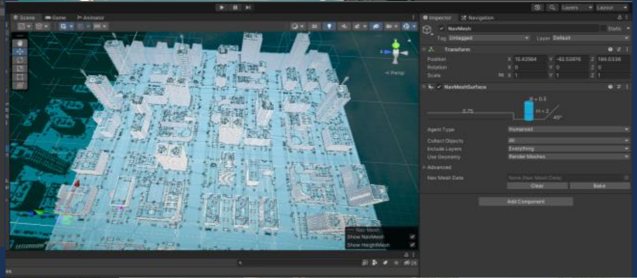

ESCAPE AND EXPLOITATIONS
BROAD TARGET SELECTION
INTELLIGENCE AND SURVEILLANCE
SPECIFIC TARGET SELECTION
PRE-ATTACK SURVEILLANCE AND PLANNING
ATTACK REHEARSAL
ACTION ON THE OBJECTIVE

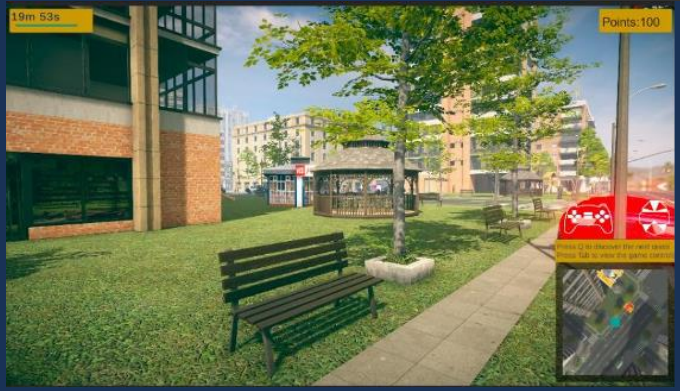
VR Game Artifacts

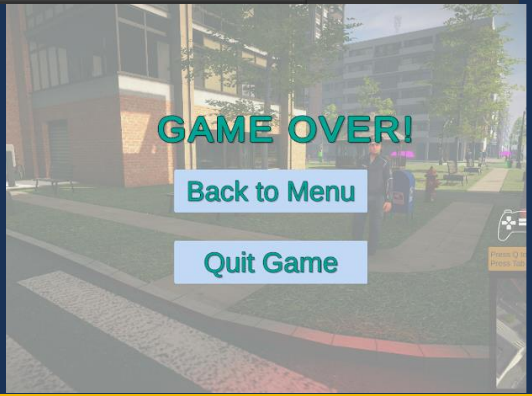
- Objects of the VR Environment
- Quests
- Game Management and Control
- Scoring
- Time Management
- Data Generation





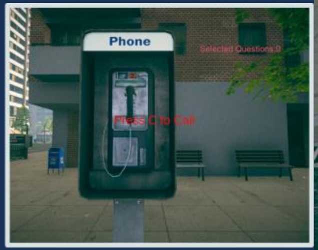






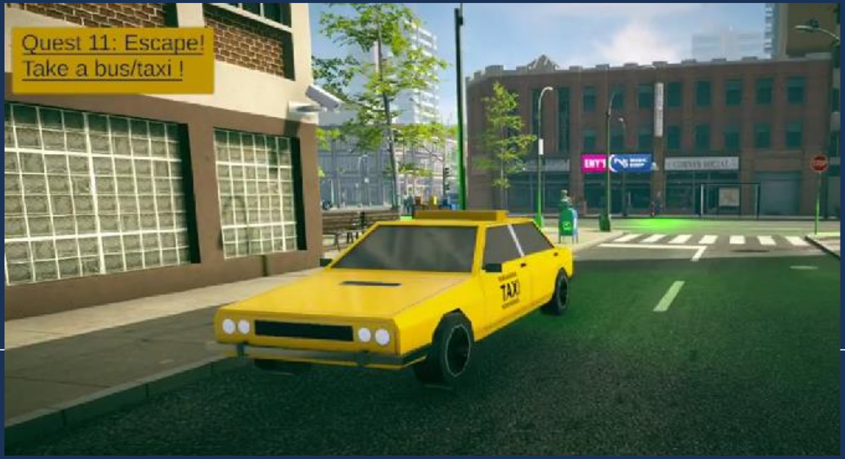
Objects of the VR Environment

- Buildings
- Cameras
- Waypoints
- Phone
- Kiosks
- Police Station
- Safehouse
- Non-Playable Characters
- ….

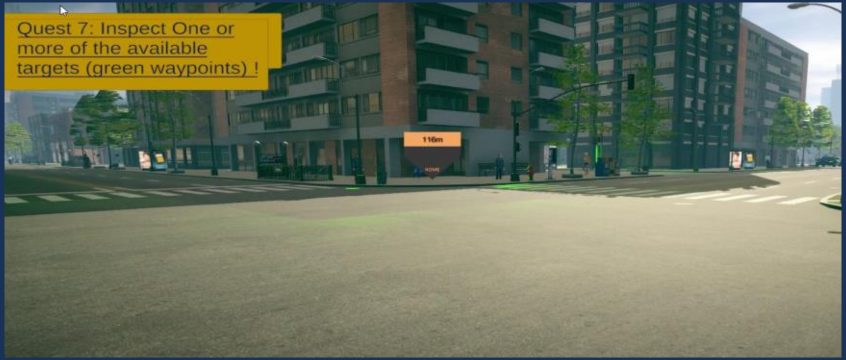


Examples of Quests

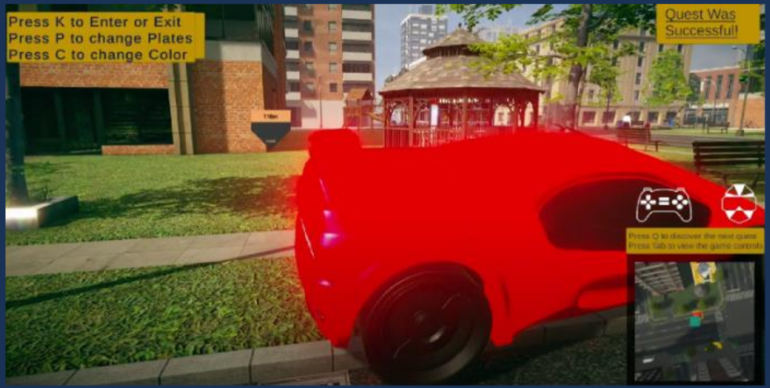
- Quest 1: Locate and inspect safehouse location (orange waypoint)
- Quest 2: Check MiniMap and acquire supplies (pink box)
- Quest 3: Deliver the materials to the Safehouse (orange waypoint)
- Quest 4: Call one of your partners using the phone booth outside the safehouse
- Quest 5: Change Car Plates
- Quest 6: Enter the car to drive around
- Quest 7: Inspect One or more of the available targets (green waypoints)
- Quest 8: Go back and enter inside the safehouse to prepare a bomb
- Quest 9: Approach one of the available targets and place the bomb
- Quest 10: Buy an evasion ticket at the kiosk
- Quest 11: Escape! Take a bus/taxi



Quest 11: Escape!
Take a bus/taxi !



Quest 7: Inspect One or more of the available targets (green waypoints) !



Press K to Enter or Exit
Press P to change Plates
Press C to change Color

Quest Was Successful!

Press Q to discover the next quest
Press Tab to view the game controls

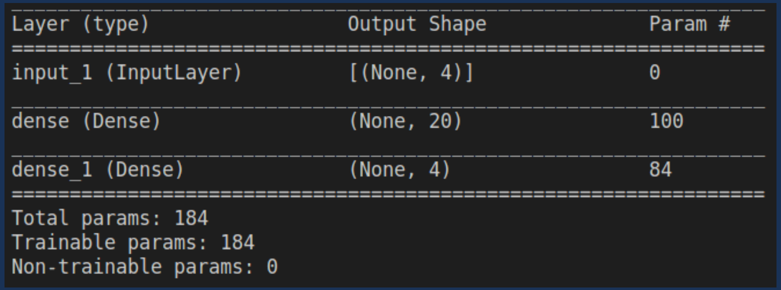
Data Generation

- Player Movements + “Noise”
- Game actions
- Surveillance objects
- Avatar moves
- NPC$_k$ moves (with K>=1 and K<=N) i.e., N tables with the movements (e.g., trajectories) of each NPC

Code	Actions
1FT	Foot surveillance (e.g., via LEA patrols or Cameras or helicopters)
5AS	Acquiring supplies
4IS	Information seeking (e.g., Phone Booth, actions near field of view of NPCs)
2VCP	Attach vehicle plates
3VCP	Remove vehicle plates
4VCP	Place new vehicle plates
3VS	Enter the vehicle
6TA	Test alarms
8PB	Prepare bomb
9PB	Place bomb
7BET	Buy evasion tickets (e.g., vending kiosk locations)
10ETP	Escape from the target

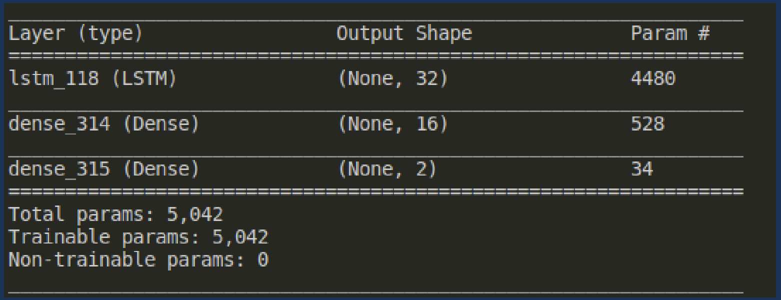
From Generated Data to AI (Deep learning) Development

Autoencoders



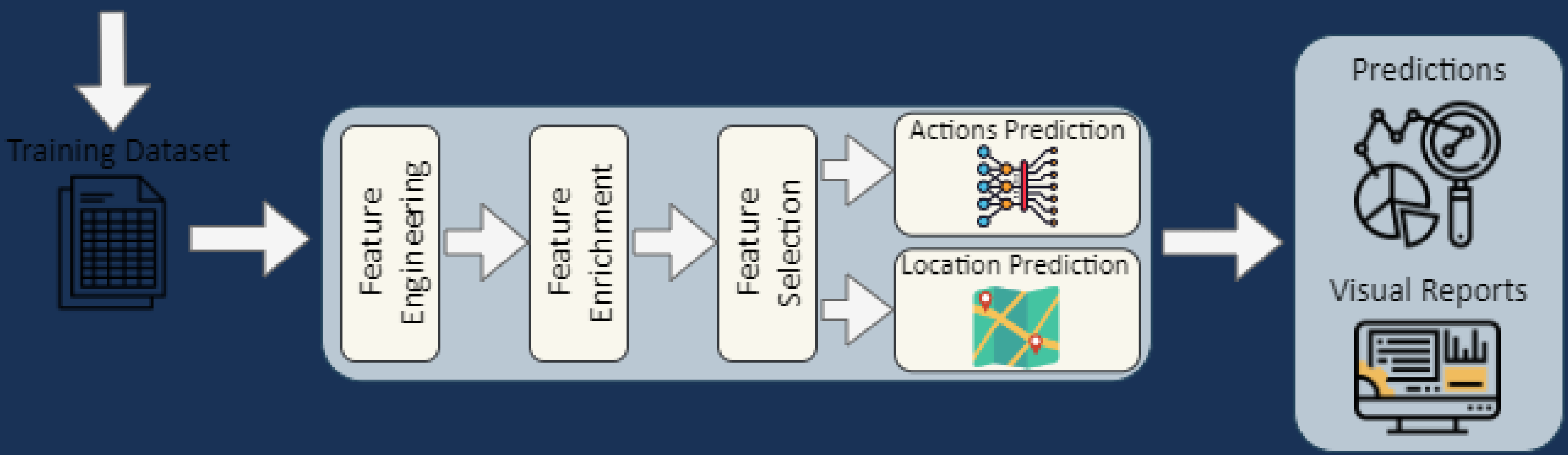
```
Layer (type)                 Output Shape              Param #
=================================================================
input_1 (InputLayer)         [(None, 4)]               0
_________________________________________________________________
dense (Dense)                (None, 20)                100
_________________________________________________________________
dense_1 (Dense)              (None, 4)                 84
=================================================================
Total params: 184
Trainable params: 184
Non-trainable params: 0
```

LSTM



```
Layer (type)                 Output Shape              Param #
=================================================================
lstm_118 (LSTM)              (None, 32)                4480
_________________________________________________________________
dense_314 (Dense)            (None, 16)                528
_________________________________________________________________
dense_315 (Dense)            (None, 2)                 34
=================================================================
Total params: 5,042
Trainable params: 5,042
Non-trainable params: 0
_________________________________________________________________
```

Serious Game



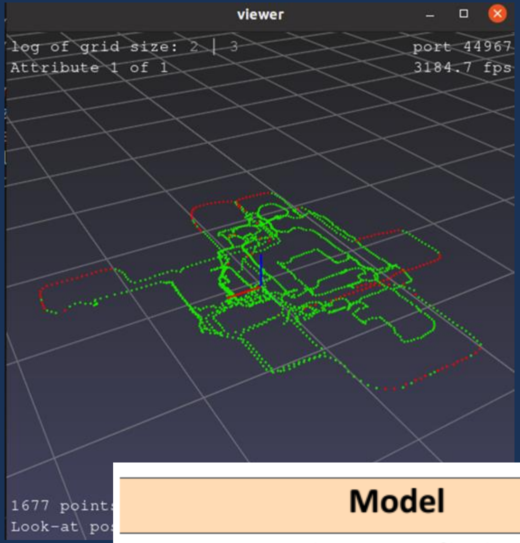
AI Integration & Preliminary Results

1. Classification of Abnormal Behaviours

2. Prediction of the Location of the Terrorist

3. Integration with the Game to Offer Increased Intelligence to the Players (Insights) or the Game Engine (Configure Difficulty Levels)

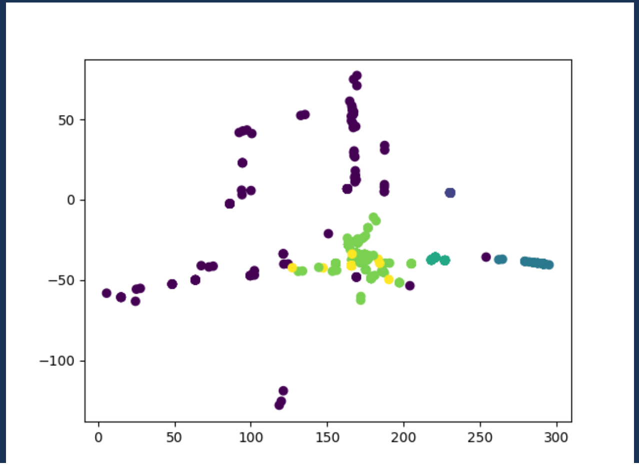
Trajectory of Terrorist



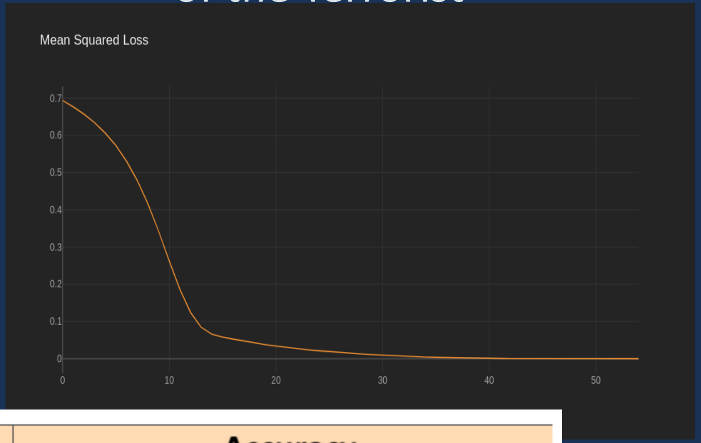
```
log of grid size: 2 | 3                port 44967
Attribute 1 of 1                       3184.7 fps

1677 point
Look-at po
```

DBSCAN for Noise Classification



Prediction of Next Location of the Terrorist



Model	Loss	Accuracy
Actions Prediction	0.013 (RMSE)	86.84%
Next Location Prediction	0.005 (RMSE)	0.005 (RMSE)

AGENDA

01 LAW-GAME Project Overview

02 Use of AI in LAW-GAME

03 AI for Predicting Indicators of Terroristic Attacks

04 Measures for Bias Alleviation & AI Act Compliance

05 How LAW-GAME helps LEAs with AI Bias

The (“Artificial Intelligence Act –AIA”)

Suite of new legislative and non-legislative proposals related to artificial intelligence (AI)

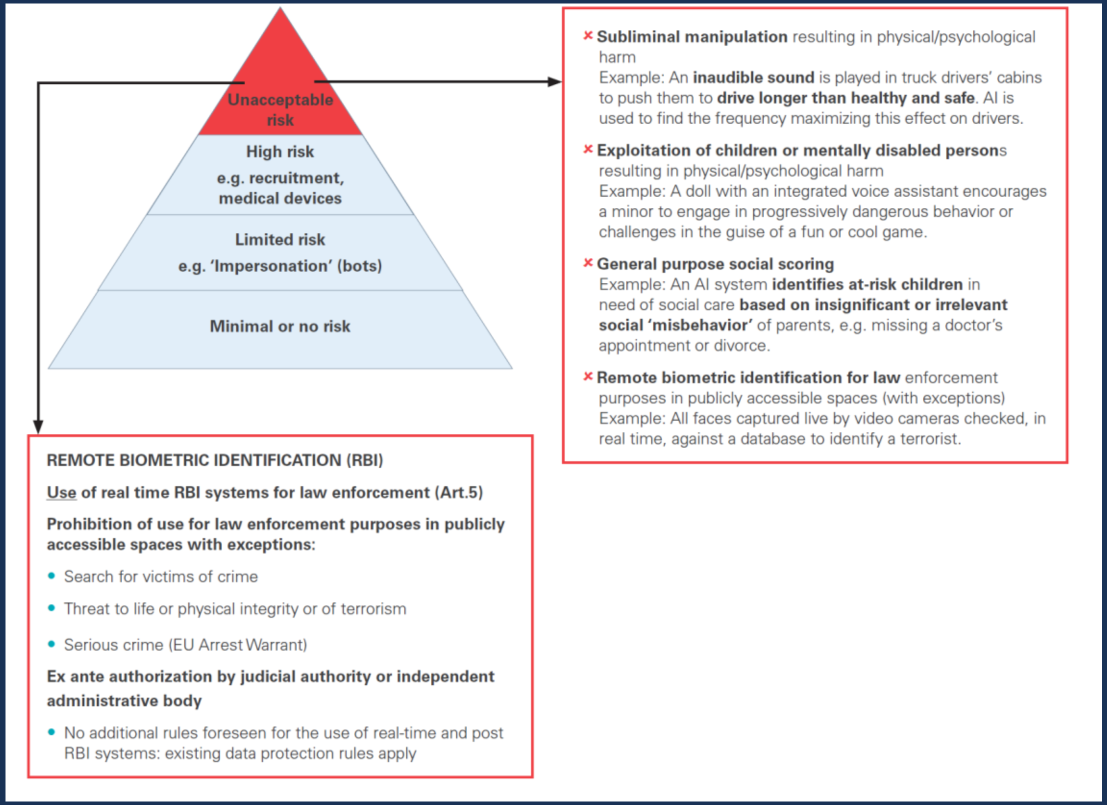
- The first-ever comprehensive legal framework

The proposed AIA is accompanied by a revised AI Coordination Plan with member states (Plan)

- Aims to “accelerate, act and align AI policy priorities and investments across Europe”.

Existing/planned projects related to AI at the EU level, as well as the various funding opportunities, including via the new Recovery and Resilience Facility

Risk Based Categorization of AI Systems: Unacceptable Risk



Unacceptable risk

High risk
e.g. recruitment, medical devices

Limited risk
e.g. 'Impersonation' (bots)

Minimal or no risk

- × **Subliminal manipulation** resulting in physical/psychological harm
  Example: An **inaudible sound** is played in truck drivers' cabins to push them to **drive longer than healthy and safe**. AI is used to find the frequency maximizing this effect on drivers.
- × **Exploitation of children or mentally disabled person**s resulting in physical/psychological harm
  Example: A doll with an integrated voice assistant encourages a minor to engage in progressively dangerous behavior or challenges in the guise of a fun or cool game.
- × **General purpose social scoring**
  Example: An AI system **identifies at-risk children** in need of social care **based on insignificant or irrelevant social 'misbehavior'** of parents, e.g. missing a doctor's appointment or divorce.
- × **Remote biometric identification for law** enforcement purposes in publicly accessible spaces (with exceptions)
  Example: All faces captured live by video cameras checked, in real time, against a database to identify a terrorist.

REMOTE BIOMETRIC IDENTIFICATION (RBI)

Use of real time RBI systems for law enforcement (Art.5)

Prohibition of use for law enforcement purposes in publicly accessible spaces with exceptions:

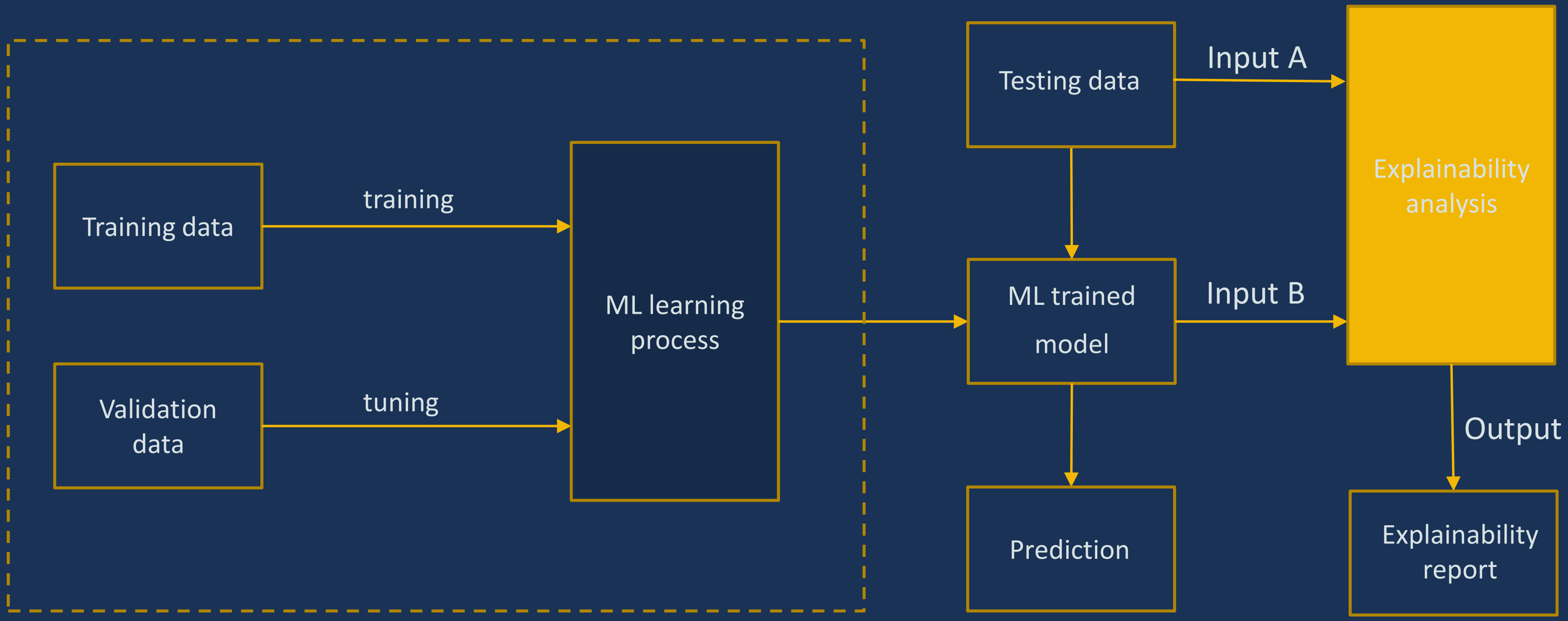
- Search for victims of crime
- Threat to life or physical integrity or of terrorism
- Serious crime (EU Arrest Warrant)

Ex ante authorization by judicial authority or independent administrative body

- No additional rules foreseen for the use of real-time and post RBI systems: existing data protection rules apply

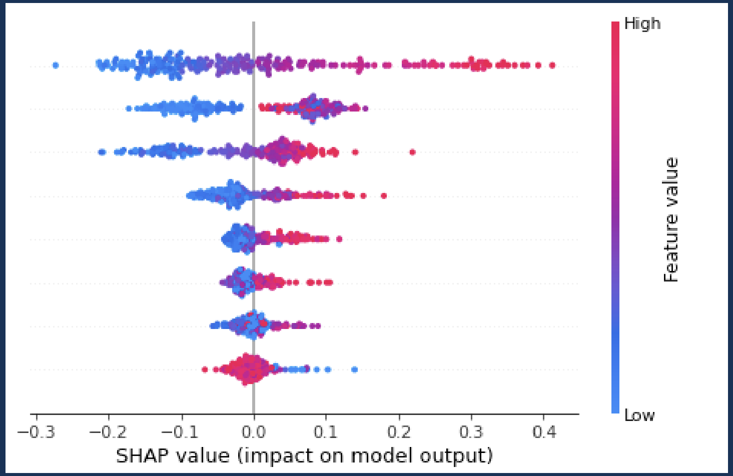
Source: DG CNECT Presentation 8 June 2021, edited by Squire Patton Boggs

High Level Architecture for AI Explanations



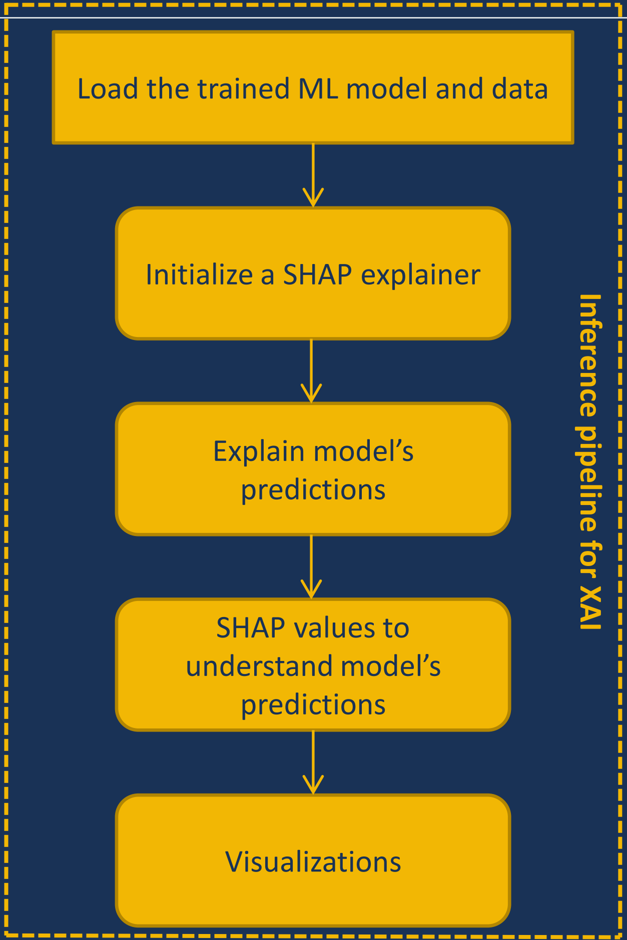
AI models explainability

- Explain AI Modules/Functions:
  - Why an Avatar is suspicious?
  - Why a location is associated with terroristic activity?
- Use XAI insight to provide more information to users:
  - Increase transparency of the AI modules and the users' trust on their recommendations
- **Explainability tools**
  - SHAP (SHapley Additive exPlanations)
  - LIME (Local Interpretable Model Agnostic Explanation)
  - gLIME (graphical LIME, a novel more intuitive version of LIME)



Multi-Level AI Explainability

- Main levels
  - Game level:
    - All avatars in the game:
      - *Beeswarm summary plots*
      - *Dependence plots*
  - User level
    - Specific avatar's behavioral patterns:
      - *Decision plots*
      - *Violin summary plots*
  - Time instance level
    - Avatar's specific actions at a time instance:
      - *Force plots*
      - *Decision plots*


Load the trained ML model and data
Initialize a SHAP explainer
Explain model's predictions
SHAP values to understand model's predictions
Visualizations
Inference pipeline for XAI

AGENDA

01 LAW-GAME Project Overview

02 Use of AI in LAW-GAME

03 AI for Predicting Indicators of Terroristic Attacks

04 Measures for Bias Alleviation & AI Act Compliance

05 How LAW-GAME helps LEAs with AI Bias

Conclusion: How LAW-GAME helps LEAs with AI Analytics and Bias

1. Ensuring Data Availability: Trusted Data Generation
2. Data Trustworthiness: Data Reliability through Provenance & Traceability
3. AI Transparency & Explainability: XAI Techniques
4. Human Oversight - Final Decision
5. Lower Risk Gamified Virtual Environment

Thank you for your attention!

QUESTIONS?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No 101021714.

STARLIGHT project

Ezgi Eren
KU Leuven Centre for IT & IP Law – imec, Belgium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021853.

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

Ezgi Eren (KU Leuven Centre for IT & IP Law (CiTiP) – imec)

Ezgi.eren@kuleuven.be

https://starlight-h2020.eu | @starlight_h2020 | starlight@cea.fr

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

STARLIGHT Vision

"Enhance the EU's strategic autonomy in the field of artificial intelligence (AI) for law enforcement agencies (LEAs)"

✦**Challenge**: complexity and data-rich security domain

✦**Opportunity**: application of AI to LEA practices

✦**Risk:** criminal misuse of AI

✦**Goals:** improve AI capabilities, tools, and data quality

✦**Outcome:** AI autonomy and resilience in the LEA community through collaboration

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

Key Facts

Coordinator: CEA (France)

Start Date: October 2021

Duration: 48 months

52 Partners

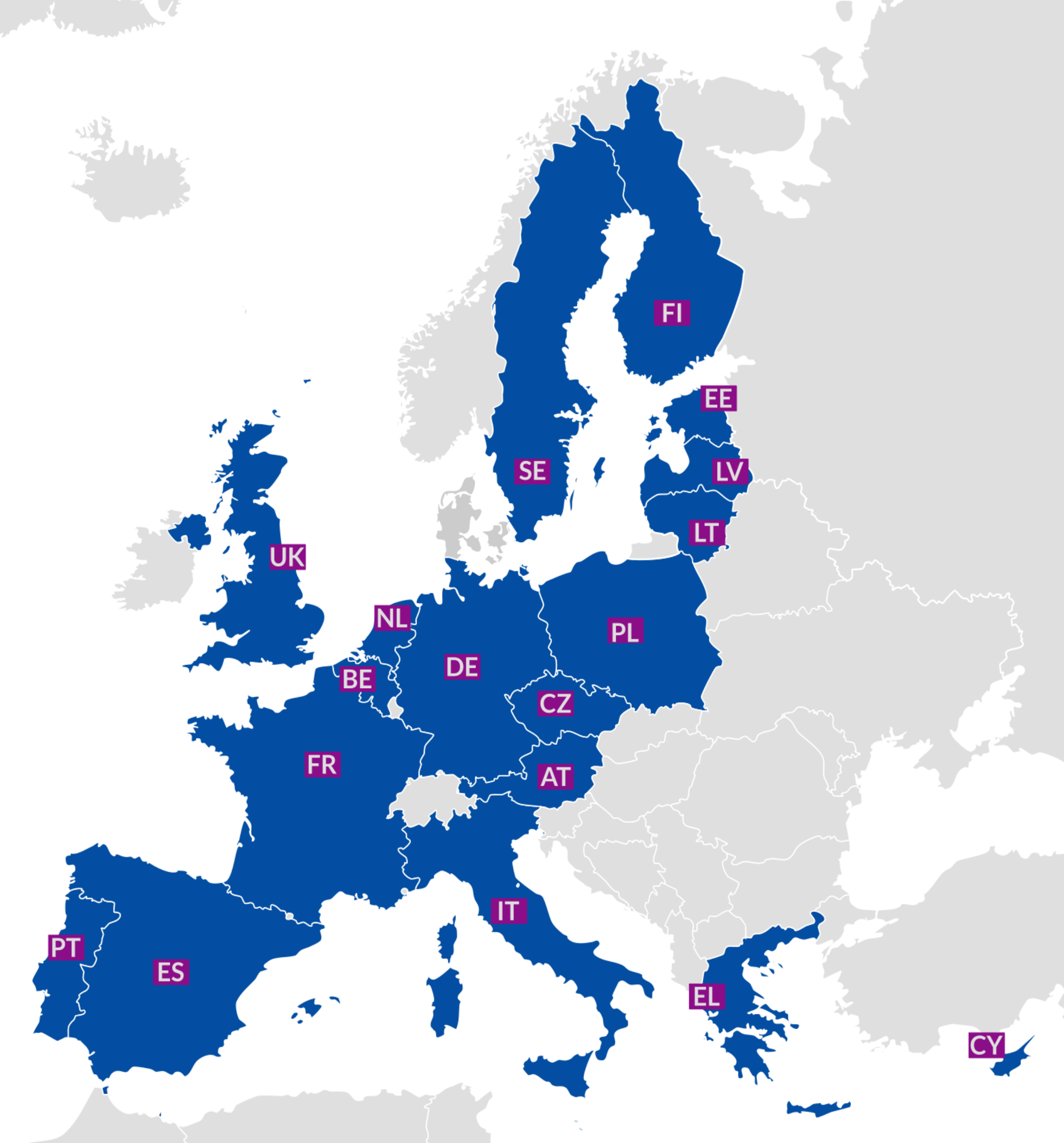
18 Countries, 15 LEAs

Call: H2020-SU-AI02-2020

Secure and resilient Artificial Intelligence technologies, tools and solutions in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence

Type: Innovation Action

Budget: €18.8m



Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

STARLIGHT Partners

list ceatech	AMS	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY	Bundesministerium Inneres	BUNDESPOLIZEI	cnrs	CFLW Cyber Strategies	Cybercrime Research Institute	ERTZAINTZA
DFK	ENGINEERING	ethics	CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS	EUROPOL	vicomtech MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE	ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ	herta	ianus consulting
inov inesc • inovação	ICCS ΕΠΙΣΕΥ	iTTi	KU LEUVEN CiTiP CENTRE FOR IT & IP LAW	KEMEA	L3CE Lithuanian Cybercrime Center of Excellence for Training, Research & Education	FONDAZIONE links PASSION FOR INNOVATION	Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE MINISTÈRE DE L'INTÉRIEUR	
GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR		MunichInnovationLabs	POLIISI	NICC INCC	TNO innovation for life	Netherlands Forensic Institute Ministry of Justice and Security	Pluribus One	Police Fédérale Federale Politie
POLICIE ČESKÉ REPUBLIKY	Polisen Swedish Police	Estonian Police and Border Guard Board	CENTRIC Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research	Stichting DITSS Dutch Institute for Technology Safety & Security	VTT	THALES	POLITIE	TILDE
FOI	voice interaction	POLITÉCNICA	10 WEB-IQ	XXII TWENTYTWO	Zentrale Stelle für Informationstechnik im Sicherheitsbereich	Police Politie		

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

STARLIGHT Approach

Create a community that brings together LEAs, researchers, industry and practitioners in the security ecosystem under a coordinated and strategic effort to bring AI into operational practices.

Improve the widespread UNDERSTANDing of AI across LEAs to reinforce their investigative and cybersecurity operations and the need to uphold legal, ethical and societal values

UNDERSTAND

Provide opportunities to LEAs to EXPLOIT AI tools and solutions in their operational work that are trustworthy, transparent and human-centric

EXPLOIT

Ensure that LEAs can PROTECT their own AI systems through privacy- and security-by-design approaches, better cybersecurity tools and knowledge

PROTECT

Raise LEAs' expertise and capacity to COMBAT the misuse of AI-supported crime and terrorism

COMBAT

BOOST AI for LEAs in Europe through high-quality datasets, an interoperable and standardised framework for long term sustainability of solutions, and the creation of an AI hub for LEAs that supports a strong AI security industry and enhances the EU's strategic autonomy in AI.

BOOST

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

Examples of STARLIGHT‘s work in Data Analytics and AI Bias in LEAs decision-making

- **WP5 focusing on data (TNO)**
  - Training/Testing Datasets fostering AI in support of LEAs
  - Specific task on data quality assessment, management and assurance
    - to provide LEAs with tools to identify bias or under-representation in a dataset, and assess the suitability of a dataset for training AI models,
    - to identify weaknesses in data or missing data groups, in order to prevent inappropriate use of data for model training and avoid problems of bias and discrimination in developed tools.
  - Continous technical, legal and ethics assessment of datasets to prevent bias

Introduction to STARLIGHT

Sustainable Autonomy and Resilience for LEAs Using AI Against High Priority Threats

Examples of STARLIGHT‘s work in Data Analytics and AI Bias in LEAs decision-making

- **WP4 & WP12 focusing on ethical and legal aspects**
  - Research task concerning „Multidisciplinary Perspectives on Algorithmic Bias“ **(Plus Ethics)**
  - Continous guidance and monitoring to avoid bias in the AI tools that STARLIGHT partners are developing
  - Ethical and Legal Observatory

- **Collaboration with AP4AI (CENTRIC and EUROPOL)**
  - Self-assessment tool including elements to assess bias, to be implemented within STARLIGHT

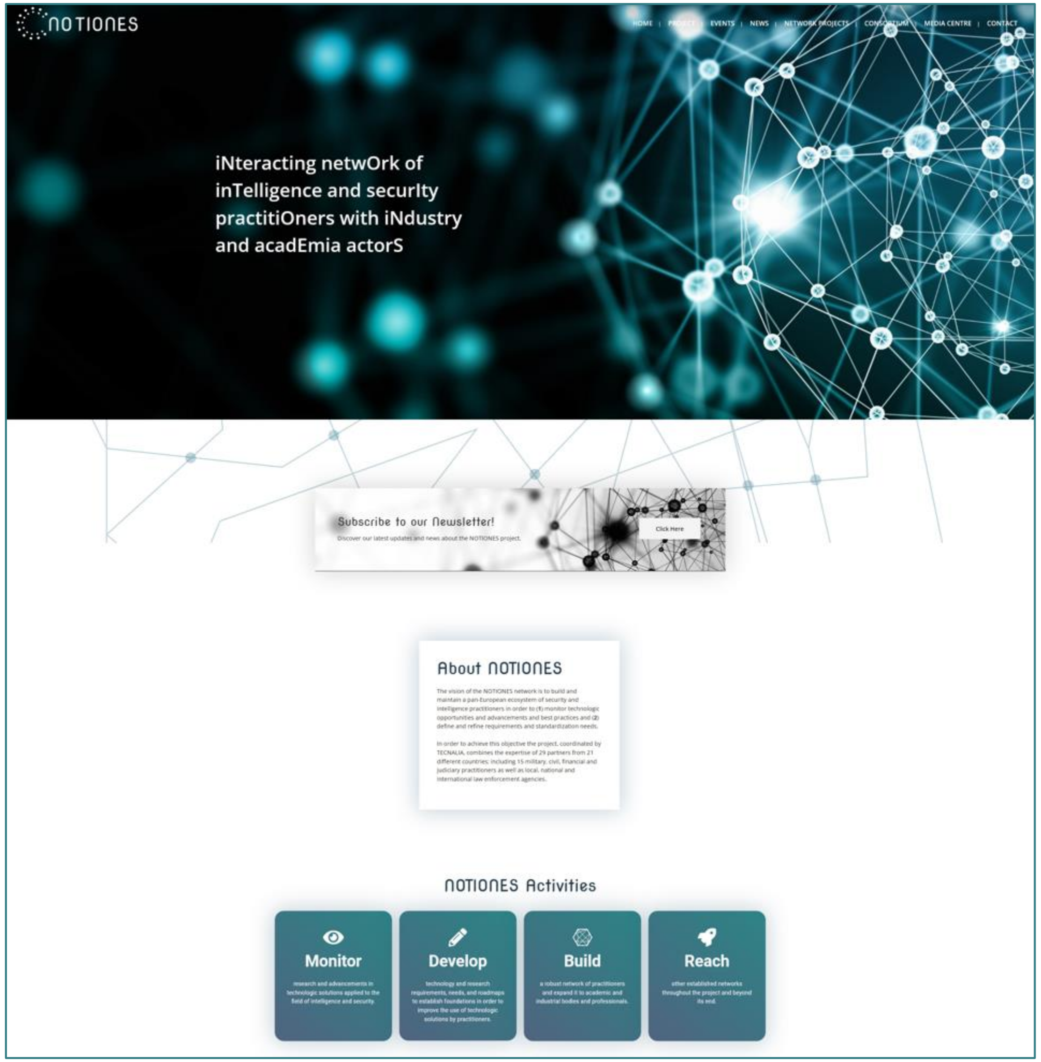
Questions & Answers

Ezgi Eren (KU Leuven Centre for IT & IP Law (CiTiP) – imec)

Ezgi.eren@kuleuven.be

DISSIMINATION & COMMUNICATION

Project website https://www.notiones.eu



NOTIONES

HOME | PROJECT | EVENTS | NEWS | NETWORK PROJECTS | CONSORTIUM | MEDIA CENTRE | CONTACT

iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS

Subscribe to our Newsletter!

Discover our latest updates and news about the NOTIONES project.

Click Here

About NOTIONES

The vision of the NOTIONES network is to build and maintain a pan-European ecosystem of security and intelligence practitioners in order to (1) monitor technologic opportunities and advancements and best practices and (2) define and refine requirements and standardization needs.

In order to achieve this objective the project, coordinated by TECNALIA, combines the expertise of 29 partners from 21 different countries; including 15 military, civil, financial and judiciary practitioners as well as local, national and international law enforcement agencies.

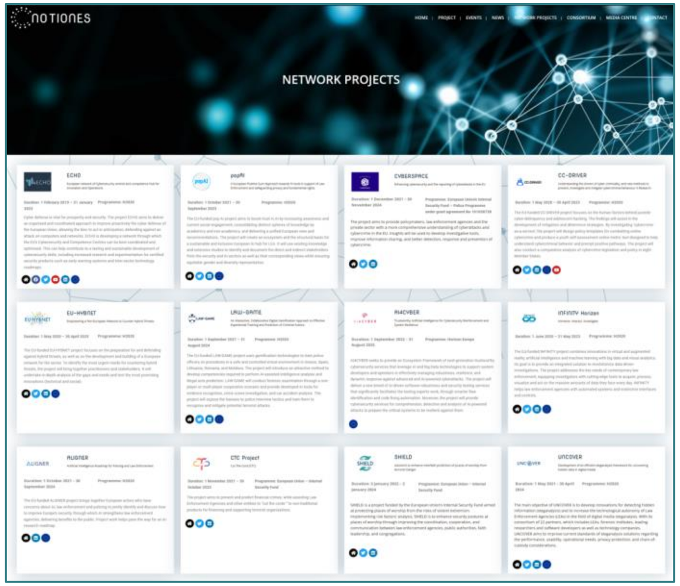
NOTIONES Activities

Monitor research and advancements in technologic solutions applied to the field of intelligence and security.

Develop technology and research requirements, needs, and roadmaps to establish foundations in order to improve the use of technologic solutions by practitioners.

Build a robust network of practitioners and expand it to academic and industrial bodies and professionals.

Reach other established networks throughout the project and beyond its end.



NOTIONES

HOME | PROJECT | EVENTS | NEWS | NETWORK PROJECTS | CONSORTIUM | MEDIA CENTRE | CONTACT

NETWORK PROJECTS

ECHO

popAI

CYBERSPACE

CC-DRIVER

EU-HYBNET

LAW-GAME

AI4CYBER

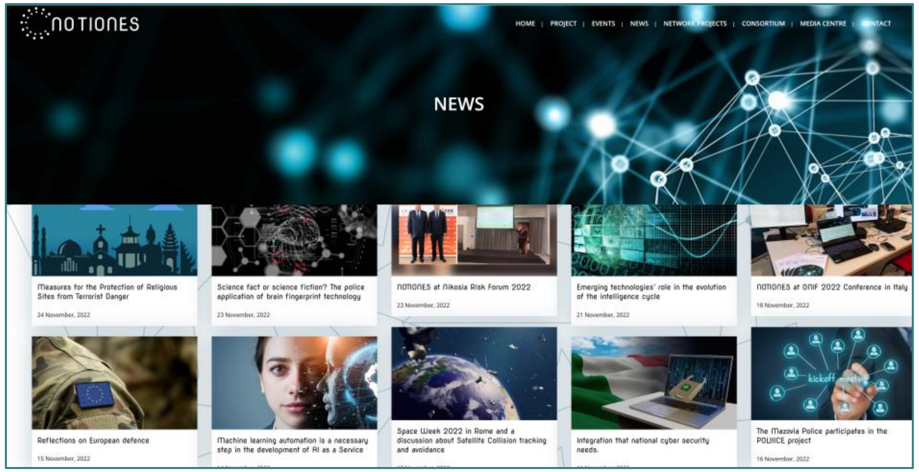
INFINITY Horizon

ALIGNER

CTC Project

SHIELD

UNCOVER



NOTIONES

HOME | PROJECT | EVENTS | NEWS | NETWORK PROJECTS | CONSORTIUM | MEDIA CENTRE | CONTACT

NEWS

Measures for the Protection of Religious Sites from Terrorist Danger

24 November, 2022

Science fact or science fiction? The police application of brain fingerprint technology

23 November, 2022

NOTIONES at Nikosia Risk Forum 2022

23 November, 2022

Emerging technologies' role in the evolution of the intelligence cycle

21 November, 2022

NOTIONES at ONIF 2022 Conference in Italy

18 November, 2022

Reflections on European defence

15 November, 2022

Machine learning automation is a necessary step in the development of AI as a Service

Space Week 2022 in Rome and a discussion about Satellite Collision tracking and avoidance

Integration that national cyber security needs.

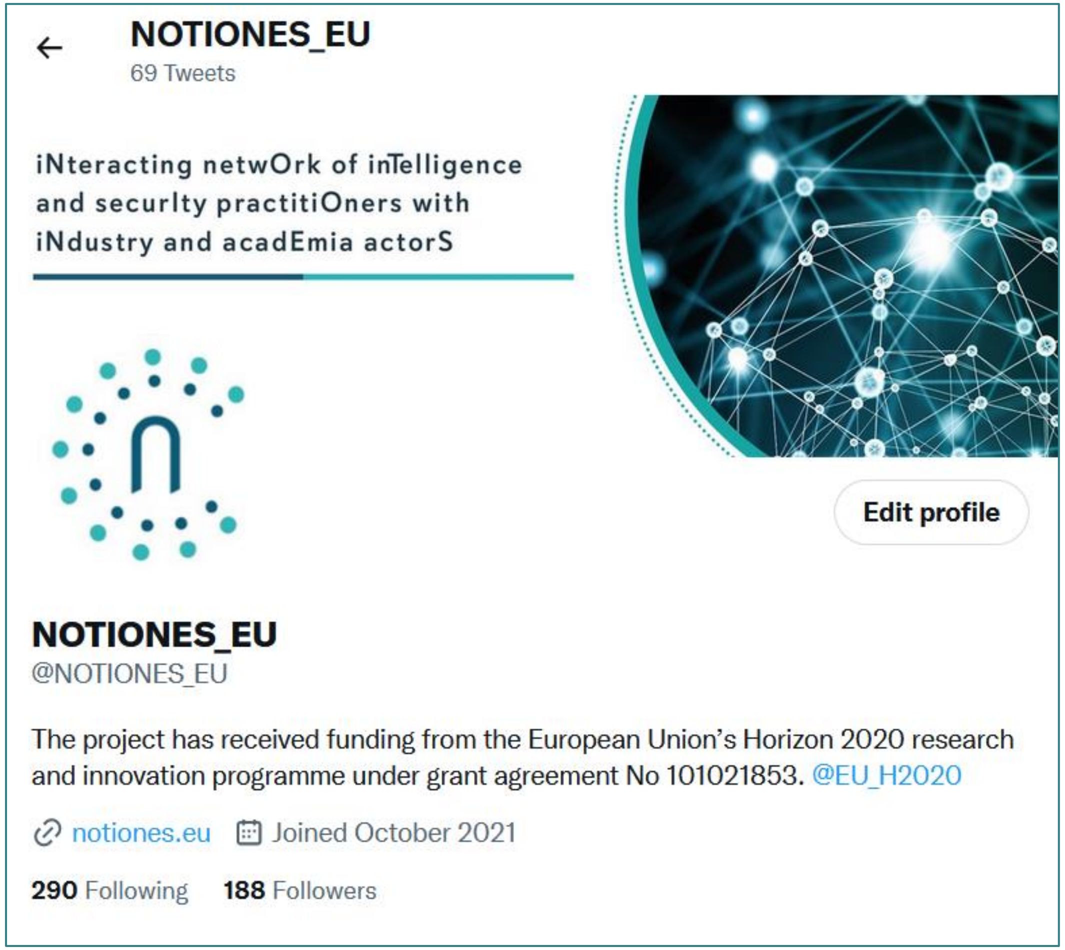
The Mazovia Police participates in the POLIICE project

16 November, 2022

Scan Me

DISSIMINATION & COMMUNICATION

Twitter account | https://twitter.com/NOTIONES_EU



← NOTIONES_EU

69 Tweets

iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS

NOTIONES_EU

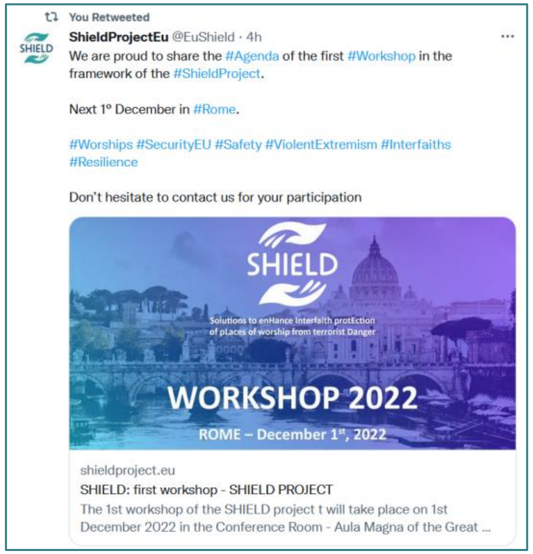
@NOTIONES_EU

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853. @EU_H2020

notiones.eu Joined October 2021

290 Following 188 Followers

Scan Me



You Retweeted

ShieldProjectEu @EuShield · 4h

We are proud to share the #Agenda of the first #Workshop in the framework of the #ShieldProject.

Next 1° December in #Rome.

#Worships #SecurityEU #Safety #ViolentExtremism #Interfaiths #Resilience

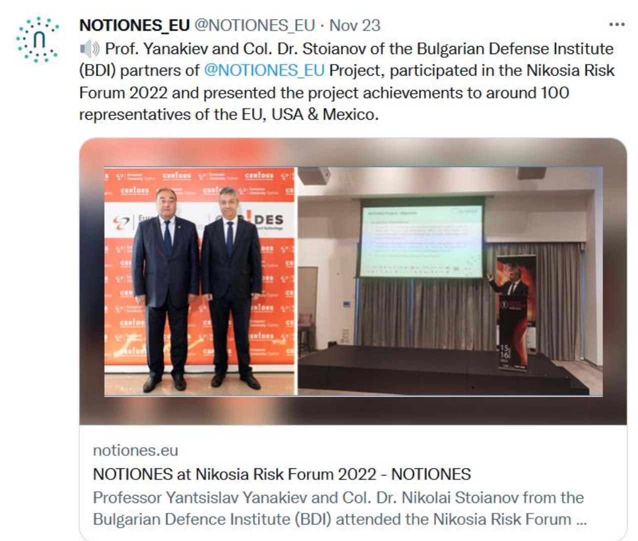
Don't hesitate to contact us for your participation

SHIELD
Solutions to enHance Interfaith protEction of pLaces of worship from terrorist Danger
WORKSHOP 2022
ROME – December 1st, 2022

shieldproject.eu

SHIELD: first workshop - SHIELD PROJECT

The 1st workshop of the SHIELD project t will take place on 1st December 2022 in the Conference Room - Aula Magna of the Great ...



NOTIONES_EU @NOTIONES_EU · Nov 23

🔈 Prof. Yanakiev and Col. Dr. Stoianov of the Bulgarian Defense Institute (BDI) partners of @NOTIONES_EU Project, participated in the Nikosia Risk Forum 2022 and presented the project achievements to around 100 representatives of the EU, USA & Mexico.

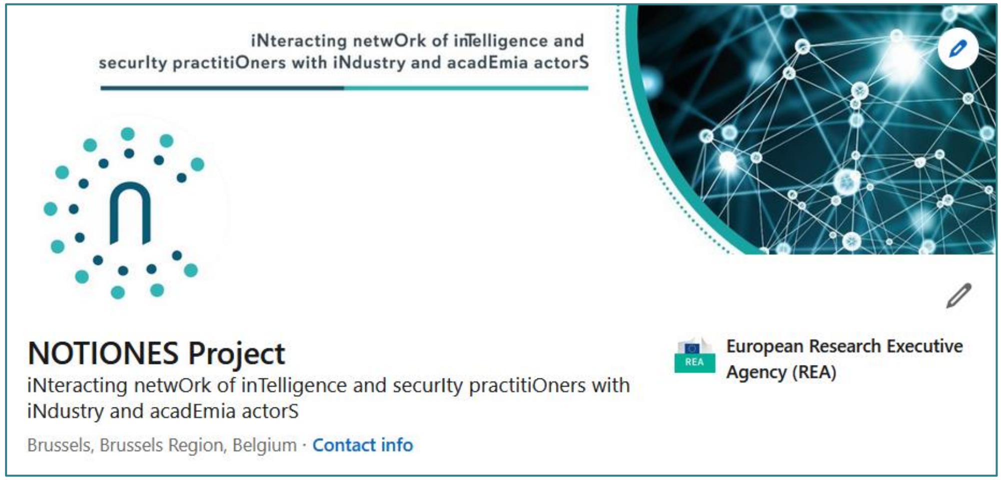
notiones.eu

NOTIONES at Nikosia Risk Forum 2022 - NOTIONES

Professor Yantsislav Yanakiev and Col. Dr. Nikolai Stoianov from the Bulgarian Defence Institute (BDI) attended the Nikosia Risk Forum ...

DISSIMINATION & COMMUNICATION

LinkedIn account | https://www.linkedin.com/in/notiones-project-93aa22224/



iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS

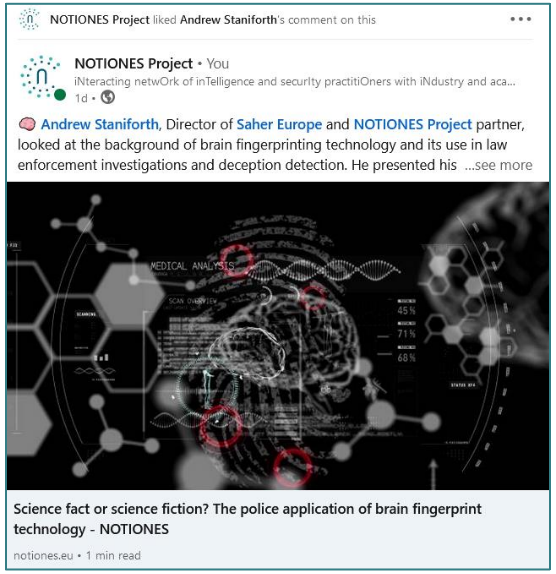
NOTIONES Project

iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS

Brussels, Brussels Region, Belgium · Contact info

European Research Executive Agency (REA)

Scan Me in



NOTIONES Project liked Andrew Staniforth's comment on this

NOTIONES Project • You
iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and aca...
1d •

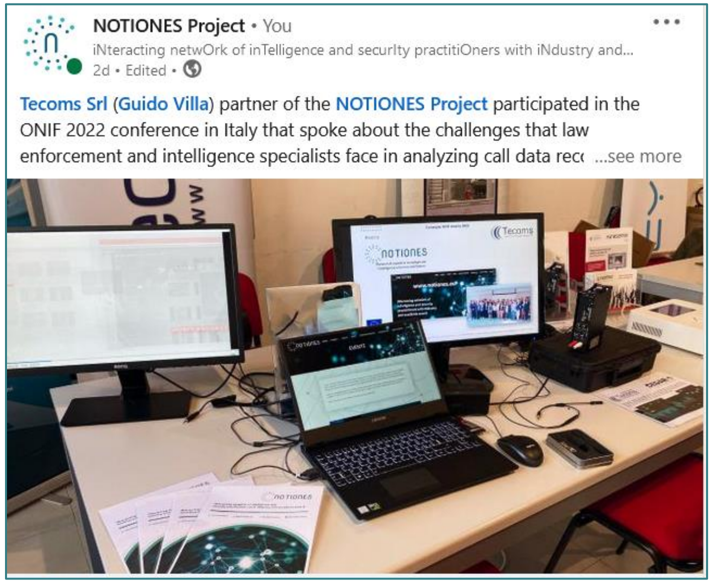
Andrew Staniforth, Director of Saher Europe and NOTIONES Project partner, looked at the background of brain fingerprinting technology and its use in law enforcement investigations and deception detection. He presented his ...see more

Science fact or science fiction? The police application of brain fingerprint technology - NOTIONES
notiones.eu • 1 min read

NOTIONES Project likes this

CTC Project
211 followers
1d •

With the CTC Project glossary until now we have explored the definitions of:
FinTech
Cryptocurrency ...see more



NOTIONES Project • You
iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and...
2d • Edited •

Tecoms Srl (Guido Villa) partner of the NOTIONES Project participated in the ONIF 2022 conference in Italy that spoke about the challenges that law enforcement and intelligence specialists face in analyzing call data rec ...see more

Thank you for your attention!
Contact us, get involved, stay updated:

office@notiones.eu

www.notiones.eu

@NOTIONES_EU

NOTIONES