NOTIONES

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

D5.2

Monitoring of EU Research and Horizon Scanning -v1

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

Project Details

Acronym: **NOTIONES**

Title: **iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS**

Coordinator: **FUNDACIÓN TECNALIA RESEARCH & INNOVATION** (SPAIN)

Reference: 101021853

Type: Coordination and support action

Program: HORIZON 2020

Theme: Pan-European networks of practitioners and other actors in the field of security

Topic-ID: SU-GM01-2020

Start: 01.09.2021 – 31.08.2026

Duration: 60 months

Consortium:

Id	Participant Name	Short name	Country
1	FUNDACIÓN TECNALIA RESEARCH & INNOVATION	TECNA	Spain
2	ZANASI ALESSANDRO SRL	Z&P	Italy
3	LAUREA UNIVERSITY OF APPLIED SCIENCES LTD	LAU	Finland
4	BULGARIAN DEFENCE INSTITUTE	BDI	Bulgaria
5	DEFENCE RESEARCH INSTITUTE	DRI	France
6	FONDAZIONE ICSA – INTELLIGENCE CULTURE AND STRATEGIC ANALYSIS	ICSA	Italy
7	BAR ILAN UNIVERSITY EUROPE INSTITUTE	BIU	Israel
8	AGENCY FOR THE PROMOTION OF EUROPEAN RESEARCH	APRE	Italy
9	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	Finland
10	Expert.AI SPA	EXP.AI	Italy
11	SAHER EUROPE	SAHER	Estonia
12	MARKETSCAPE A/S	MS	Denmark
13	TECOMS SRL	TECOMS	Italy
14	SYNYO GmbH	SYNYO	Austria
15	REGIONAL POLICE HEADQUARTERS IN RADOM	KWPR	Poland
16	BULGARIAN STATE AGENCY FOR NATIONAL SECURITY	DANS	Bulgaria
17	CARABINIERI LT.GENERAL LEONARDO LESO	LESO	Italy
18	FINANCIAL INTELLIGENCE UNIT OF LATVIA	FIU	Latvia
19	BORDER POLICE OF BOSNIA HERZEGOVINA	BHBP	Bosnia & Herzegovina

20	ISEM-INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE, n.p.o.	ISEMI	Slovakia
21	KHARKIV NATIONAL UNIVERSITY OF INTERNAL AFFAIRS	KhNUIA	Ukraine
22	POLITSEI.JA PIIRIVALVEAMET	EPBG	Estonia
23	MINISTRY OF INTERIOR OF GEORGIA	MIA	Georgia
24	POLICE SERVICE OF NORTHERN IRELAND	PSNI	UK
25	SWEDISH POLICE AUTHORITY	SPA	Sweden
26	POLICIA JUDICIARIA PORTUGUESE	PJ	Portugal
27	MILITARY ACADEMY "GENERL MIHAILO APOSTOLSKI" – SKOPJE	MAGMA	North Macedonia
28	HOCHSCHULE FÜR DEN ÖFFENTLICHEN DIENST IN BAYERN	HFOED	Germany
29	GOBIERNO VASCO - DEPARTAMENTO SEGURIDAD	ERTZ	Spain

Deliverable Details

Number:	**D5.2**
Title:	**Monitoring of EU Research and Horizon Scanning -v1**
Lead beneficiary:	APRE
Work package:	WP5
Dissemination level:	PU (Public)
Nature:	Report (RE)
Due date:	30th April 2022
Submission date:	**29th April 2022**
Authors:	**Claudio Testani**, APRE; **Giulia Venturi**, Z&P
Contributors:	**Maria Ustenko**, **Graziano Giorgi**, Z&P; **Lorenzo Cuoghi**, DRI
Reviewers:	**Edoardo Sponzilli**, ICSA; **Alessandro Marani,** DRI

Version History:

Date	Version No.	Author	Notes
01/03/2022	0.1	Claudio Testani (APRE), Giulia Venturi (Z&P)	Initial version with introduction and ToC draft
16/03/2022	0.2	Giulia Venturi (Z&P)	Section 1 + Section 2.1
18/03/2022	0.3	Giulia Venturi (Z&P)	Document updated to new template_v4
29/03/2022	0.4	Giulia Venturi (Z&P)	Draft of Section 2.2
06/04/2022	0.5	Claudio Testani (APRE)	Section 3 + Annex II
07/04/2022	0.6	Giulia Venturi, Maria Ustenko (Z&P), Lorenzo Cuoghi (DRI)	Executive Summary + Section 2.2 + Annex I (contribution by DRI) + Section 4
11/04/2022	0.7	Graziano Giorgi, Giulia Venturi (Z&P), Claudio Testani (APRE)	Internal review Updated executive summary
11/04/2022	0.8	Giulia Venturi (Z&P), Claudio Testani (APRE)	Document ready for review by DRI and ICSA
19/04/2022	0.9	Giulia Venturi (Z&P), Alessandro Marani (DRI)	Document updated after review by DRI

Date	Version No.	Author	Notes
20/04/2022	0.91	Giulia Venturi (Z&P), Edoardo Sponzilli (ICSA)	Document updated after review by ICSA
29/04/2022	1	Concepción Cortés (TECNA)	Review before submission and Final version

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

Disclaimer: The content of this report reflects only the authors' view. The European Commission or the Agency are not responsible for the content and any use that may be made of the information.

Table of Content

List of Figures

List of Tables

Acronyms

LEA	Law Enforcement Agency
WP	Work Package
CSA	Coordination and Support Action
EC	European Commission
SME	Small-Medium Enterprise
EPRS	European Parliamentary Research Service
GDPR	General Data Protection Regulation
AIA	Artificial Intelligence Act
FRTs	Facial Recognition Technologies
CFR	Charter of Fundamental Rights
LED	Law Enforcement Directive
AI	Artificial Intelligence
SIS	Schengen Information System
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
WST	Wearable Sensor Technology
WG	Working Group
BRT	Biometric Recognition Technology
CIT	Communication Interception Technology
SWaP	Size, Weight, and Power
CPS	Cyber Physical System
ATOL	Automated Tool for Onion Labeling
DARPA	Defence Advanced Research Projects Agency
IA	Innovation Action
RIA	Research and Innovation Action
DNM	DarkNet Market
SOCMINT	SOCial Media INTelligence
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
IND	Improvised Nuclear Device
RDD	Radiological Dispersal Device

Executive Summary

This document represents the product of tasks T5.2 "*Research monitoring on EU projects*" and T5.3 "*Research monitoring through Horizon Scanning*" of NOTIONES Work Package 5, dedicated to innovation monitoring.
The work was carried out by adopting the methodology outlined in NOTIONES deliverable D5.1 "*Methodology for Innovation Monitoring*".
The research activities and the findings are those obtained in months M7 and M8 since the beginning of the project (first run of the tasks).

Section 1 introduces the document by describing the work frame of tasks T5.2 and T5.3, and of the overall Work Package 5 of NOTIONES.

Section 2 reports on the research activities carried out in task T5.3 "*Research monitoring through horizon scanning*". The main data source used was TheLens, but also open web and CORDIS were exploited. The datasets were primarily explored with the online statistical analysis tool of TheLens. Datasets were explored searching for publications of relevance for the current NOTIONES *focus areas*. Results are reported in subsection 2.2: subsection 2.2.1 contains findings about Edge Artificial Intelligence, Biometric Recognition Technology, Wearable Sensor Technology and Internet of Things, while subsection 2.2.2 contains findings related to the Dark Net.

Section 3 reports on the research activities carried out in task T5.2 "*Research monitoring on EU projects*. The preliminary dataset retrieval was obtained by searching on the CORDIS database the research projects mentioning keywords relevant to NOTIONES. Then, two further selection stages were performed to identify the most interesting projects in terms of relevance for the *Dark Web* focus area, relevance for the *Analysis phase of the intelligence cycle* focus area, and technology innovation (produced software or modelling), reported in subsections 3.2.1, 3.2.2 and 3.2.3, respectively. Subsection 3.2.3 presents a brief statistical analysis with regard to budget and countries distribution.

Section 4 contains a summary of the most relevant findings of both tasks T5.2 and T5.3 through the common layout for the summarisation of the information proposed in deliverable D5.1. The following technologies are presented and their possible exploitation in NOTIONES is proposed:

- the platform developed by project CONNEXIONs, dedicated to the fight of radicalisation on surface/deep/dark web as well as in social media content in seven languages;
- the INVISO platform developed by project INSIKT, that detects and foresees online radicalization;
- the Web-I-Qube hardware/software solution developed by Mh SERVICE, that performs analysis of darknet content (related to project DAN);
- the Edge AI technology, which allows to collect and process data locally, instead of in the *cloud;*
- the Biometric Recognition Technology, powered by Artificial Intelligence, and the example of the SiiP platform used by INTERPOL;
- the Wearable Sensor Technology with the example of the BorderSens project;
- brief insights on IoT hacking, interception and forensics and on Dark Web threat categorization.

Section 5 contains conclusive considerations and next steps.

1. Introduction

This document represents the product of the first run of tasks T5.2 and T5.3 of NOTIONES Work Package 5. In the next sections, the background about the project is presented (sub section 1.1), together with an overview on the specific Work Package (subsection 1.2). The structure of the document is explained in subsection 1.3.

1.1 Background

NOTIONES (iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS) is a CSA (Coordination and Support Action) project, funded by the European Commission (EC), and aims to facilitate the supply side - academia, SMEs, and research centres - and demand side - security and intelligence practitioners - of Security innovation meet.

The project results are expected to strengthen the European integration in the fields of Security and Intelligence, identifying the needs of Intelligence and Security practitioners as a result of the following:

- depicting the constraints, needs and requirements of intelligence (WP2);
- researching the state-of-the-art of technologic advancements exploitable by intelligence and security practitioners (WP3);
- analysing the changing technological terror threats facing intelligence services in Europe (WP4);
- innovation monitoring (WP5);
- gathering the expertise of academies and industries and promoting interaction with the intelligence and security practitioners (WP6);
- organising workshops and conferences to support the development of a European community of professionals dedicated to addressing long-standing intelligence challenges (WP7).

At present time (M8), the activities of WP2, WP3 and WP4 are about to end or have already ended.

On the other hand, the activities of **WP5, WP6 and WP7 are in the process of completing the first iteration of their 6-months long cycle**, as depicted in the figure below:

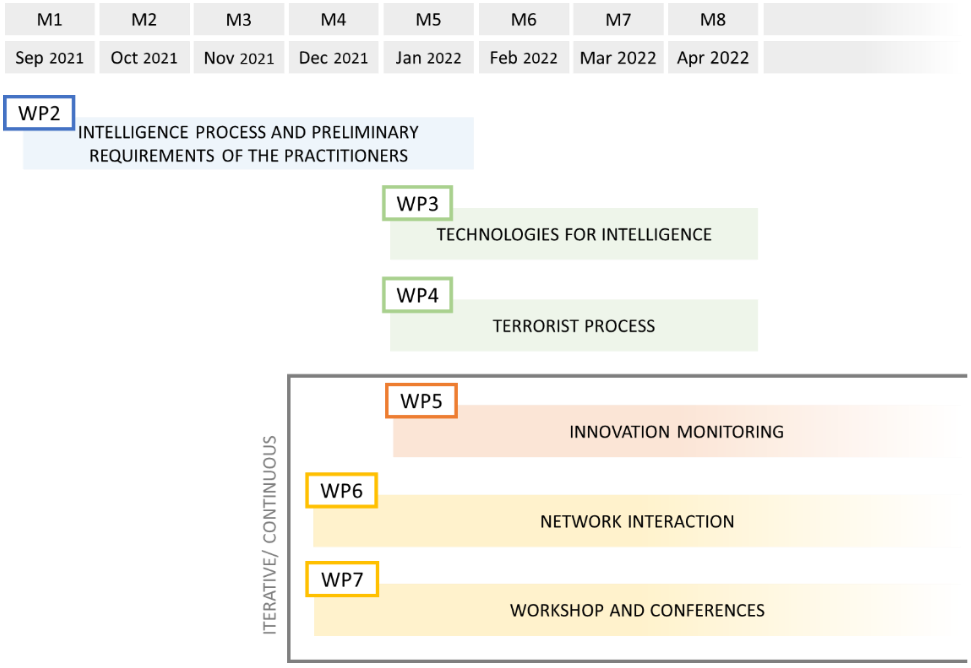


Figure 1: Time diagram of the NOTIONES Work Packages

1.2 Overview on NOTIONES Work Package 5

Work Package WP5 aims at identifying new technologic opportunities and terrorist threats to support the European Security Research and Innovation by providing fresh inputs to reshape its research and development activities in order to directly address the practitioners' needs.

Tasks **T5.2 "*Research monitoring on EU projects*"** and **T5.3 "*Research monitoring through Horizon Scanning*"** of WP5 are dedicated to i**nnovation monitoring**, defined as the activity aimed at gaining understanding of important technological trends, along with their Intelligence and Security implications, by finding and interpreting the available information in order to provide a concrete benefit to the NOTIONES network of stakeholders.

This document represents the **product of the first run of tasks T5.2 and T5.3** of WP5, which performed the research monitoring activities during M7 and M8, as depicted in Figure 2.

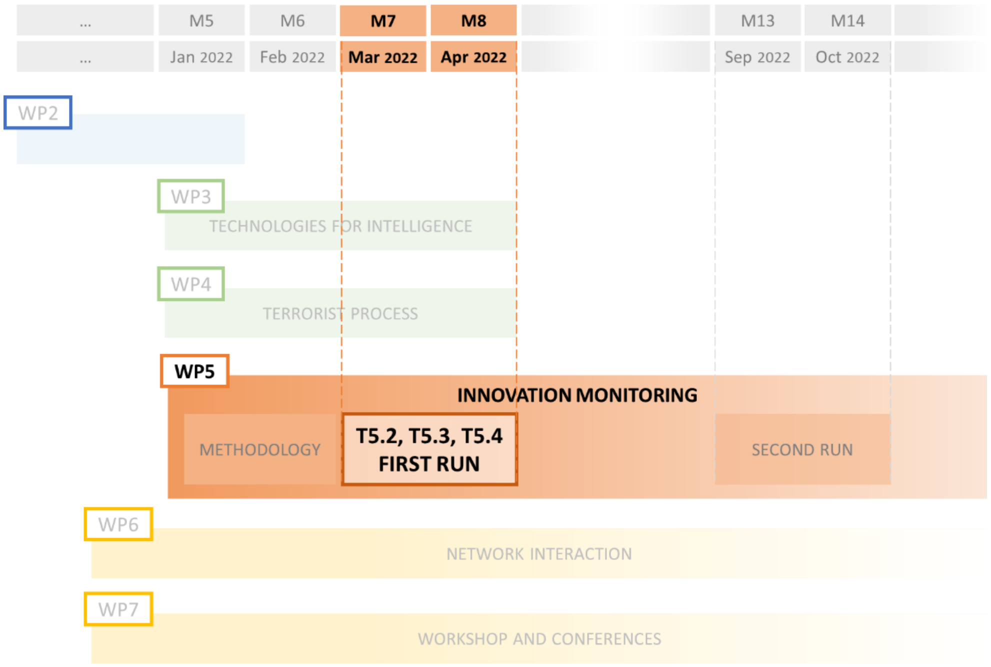


Figure 2: Time diagram of the first run of innovation monitoring in WP5

For the reader's convenience, the tasks' descriptions are recalled below:

- T5.2 Research monitoring on EU projects: this task will perform a deep survey of the emerging technologies that are the most promising in the field of intelligence and security by exploiting the great variety and volume of knowledge produced by EU research projects. To this purpose, the project will rationalize and categorize knowledge exploiting the CORDIS database as a primary source for information. In addition to this, the expertise of all NOTIONES partners will be exploited.
- T5.3 Research monitoring through Horizon Scanning: this task will perform a deep survey of the emerging technologies that are the most promising in the field of intelligence and security by exploiting the great variety and volume of knowledge openly available. To this purpose, the project will rationalize and categorize knowledge exploiting open databanks of publications and patents. The gathering of information will be performed by a targeted search based on the keywords, by means of technology horizon scanning. "Horizon scanning" is intended as systematic research of relevant technological developments with the purpose of highlighting opportunity and threats that may influence the capability of organizations and bodies providing intelligence and security services to achieve their objectives ad goals. Such analysis should also consider the maturity level of technologies, so to identify whether it is at research phase, development, prototyping or production.

It is worth reminding that task T5.4 "*Monitoring of emerging terrorist threats*" reports the findings in a separate deliverable, namely D5.11 "*Monitoring of Emerging terrorist threats -v1*".

1.3 Structure of the document

This document is structured as follows:

- Section 2 reports on the research activities carried out in task T5.3 "*Research monitoring through horizon scanning*";
- Section 3 reports on the research activities carried out in task T5.2 "*Research monitoring on EU projects*";
- Section 4 contains a summary of the most relevant findings of both tasks T5.2 and T5.3;
- Section 5 contains conclusive considerations and next steps.

As already pointed out, the research activities and the findings are those obtained from the beginning of the project up until months M7 and M8.

The methodological approach used is described in sub-sections 3.1 and 2.1, for T5.2 and T5.3 respectively, detailing the improvements and modifications applied to the general WP5 methodology encased in deliverable D5.1 "*Methodology for innovation monitoring*" (submitted in M6).

2. Research monitoring through Horizon Scanning

An essential part of the research monitoring activity is represented by Horizon Scanning, intended as a systematic research of technology trends with the purpose of highlighting opportunity and threats that may influence an organisation's capability to achieve its objectives ad goals – i.e., in NOTIONES, the security and intelligence practitioners' capability to operate.

Horizon Scanning aims at detecting new technologies, rapidly evolving and increasingly being adopted by industries, but also, in regard to already existing technologies, new combinations of such, transfer of technologies to other domains and/or new applications of existing technologies.

It can also detect the so-called emerging technologies, defined as "*a relatively fast growing and radically novel technology characterised by a certain degree of coherence persisting over time and with the potential to exert a considerable impact […] Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous*" [1]. These are very likely to be technologies at early stages of development, thus having a low Technology Readiness Level (TRL), typically at level 3 or 4 [2].

For the first run of task T5.3, Horizon Scanning was performed using a combination of techniques, taking as input the focus areas identified through interviews with the practitioners performed in WP2, and researching technologies through the analysis of free online scholar and patent databanks.

Next subsections present the methodology used (subsection 2.1), and the research description and outcomes (subsection 2.2).

2.1 Methodology

The methodology adopted for task T5.3 originates from the methodology delivered in D5.1 "Methodology for innovation monitoring". In this document it is briefly recalled it and highlighted the main modifications that were made during the work.

The idea behind the methodology is to research both, past and current information (retrieved for example through online databanks) and recognise patterns, dependencies and links among data in order to detect potential applications in the Intelligence and Security field of recently developed technologies.

The main input is represented by focus areas, intended as themes of interest, identified in WP2 and discussed within the working groups in WP6. The output is expected to be a list of promising technologies and innovations supporting practitioners in the focus areas, together with new themes for discussion. The purpose is to boost interaction between practitioners and industrial/academic stakeholders.

The main features and the methodological flow are summarized below:

- the focus areas should be broken down into key-words;
- data should be collected from selected data sources, based on aforementioned key-words;
- data should be analysed by means of iterative cycles, beginning with an exploratory desk research, to have an initial understanding of the issue under investigation, and then focusing on specific technologies or family of technologies, building a case study, or investigating an existing case study;

- minimum mandatory information should be collected for reporting the discovered technologies, plus additional information, in the same format of the NOTIONES CTI Catalogue.

The methodology was followed in its entirety in task T5.3, although some of the keywords proposed lead to no results and some adjustments were performed (see section 2.1.4).

2.1.1 Data sources and format

The main data source used was TheLens [3], using the integrated search engine on scholarly works and patents and its export functionality, which allows to export up to 50.000 results in .csv, .ris, .json or BibTeX format.

Scholarly works can be filtered by date range, flags (open access or not, has ORCID ID or not…), author, institution, institution country/region, identifier type (CrossRef, PubMed…), funding, journal, conference name, publication type (journal article, book, dissertation…), publisher, and subject matter.

Search by specific words can be performed on title, abstract, full text, keywords, and/or field of study.

The user can choose which fields should be exported among the following: title, date published, publication year, publication type, source title, ISSNs, publisher, source country, author/s, abstract, volume, issue, number, start page, end page, fields of study, keywords, mesh terms, chemicals, funding, source URLs, external URL, PMID, DOI, Microsoft Academic ID, PMCID, citing patents count, references, citing works count.

Patents can be filtered by date range, flags (has title, has abstract…), jurisdictions, applicants, inventors, owners, agents & attorneys, legal status (expired, active, pending…), document type (granted patent, patent application…), cited works, biologicals (for nucleotides and amino acids), classifications (IPC, CPCR, US classification codes), and document family (simple, extended).

Search by specific words can be performed on title, abstract, and/or claims.

The user can choose which fields should be exported among the following: jurisdiction, kind, display key, lens ID, publication date, publication year, application number, application date, priority numbers, earliest priority date, title, abstract, applicants, inventors, owners, URL, document type, has full text, cites patent count, cited by patent count, simple family size, extended family size, sequence count, CPC classifications, IPCR classifications, US classifications, NPL citation count, NPL resolved citation count, NPL resolved lens ID(s), NPL resolved external ID(s), NPL citations.

Apart from TheLens, open web and CORDIS [4] were also exploited.

2.1.2 Data analysis techniques

The datasets were primarily explored with the online statistical analysis tool of TheLens. Selected datasets were exported and processed through an internally developed Python environment which exploits the following open-source libraries:

- Dash - Python framework for analytical web apps[1];
- Pandas - Data analysis and manipulation tool[2];

[1] https://plot.ly/dash/

[2] https://pandas.pydata.org/

- NumPy - Python fundamental package for scientific computing[3];
- scikit-learn - Python machine learning library[4];
- NLTK - Natural language ToolKit library for human language data[5].

2.1.3 Profile of analyst(s)

The research was performed by Mrs. Giulia Venturi (Orcid ID: 0000-0003-0445-2613) and Miss Maria Ustenko (Orcid ID: 0000-0002-6506-7607).

Giulia holds a Master's Degree in Physics in the University of Bologna (Italy) with Internship at the University of Cambridge (UK). She is expert in technology horizon scanning and in methodologies for strategic technology foresight.

Maria holds a Bachelor in Chemistry and Master in Nanotechnology. She graduated from PFUR, Engineering Academy led by Russian Space Association. She has both academic and industrial working experiences. Currently she is working as a technical researcher in the field of Artificial Intelligence.

2.1.4 Issues encountered and search features

The methodology described in D5.1 was followed in its entirety in task T5.3, but some issues were encountered due to the specific features of the research. In the following subsections, an explanation is provided with regard to this.

2.1.4.1 Patent search

The search on patent databases for technological innovations useful for the security and intelligence practitioners proved to be difficult. The main obstacles encountered are represented by two factors.

On one side, patents are described in a very plain, simple and generic manner, avoiding details about how the patented invention will be used and by whom and focusing on the technical features that make the invention unique and original. For this reason, it is extremely unlikely to find patents directly referencing the operational environment of the invention (border control, intelligence phase…) or the possible use of the invention by specific users (LEAs, security/intelligence practitioners…).

On the other side, it is expected that the innovations of interest for NOTIONES are not specifically designed for LEAs and security/intelligence practitioners, but rather designed for civil or industrial use. Indeed, the purpose of the project is to guide the practitioners in expressing their expectations, requirements and standardisation needs about technologies so that such technologies can be successfully adapted for them.

It is therefore evident that a patent search based on the keywords "law enforcement", for instance, will result in a very poor outcome and it is necessary to first research very specific technological areas to investigate. As an example, for the sake of clarity and for the reader's convenience: with regard to border control, first there is the need to understand what are the operational capabilities that practitioners wish they could boost thanks to technology. It is assumed that practitioners are highly interested in smart devices for CBRN detection. Patent search may then be directed specifically

[3] https://numpy.org/
[4] https://scikit-learn.org
[5] https://www.nltk.org/

towards the investigation on innovative sensors for the detection of certain chemicals or certain radioisotopes.

At present time the NOTIONES Working Groups (WGs) are discussing two high-level focus areas, intended as areas where an opportunity for change, improvement or enhancement was identified, namely:

- Various challenges in monitoring and collecting data from the dark web;
- Technological needs, solutions, and improvements to the intelligence analysis phase of the intelligence cycle.

These NOTIONES task T6.1 “*First Round of Working Groups*” has not yet achieved the stage of defining specific technological areas or needs. For this reason, patent search will be postponed to the next run of task T5.3, after the WGs’ activities will have reached a higher maturity level.

2.1.4.2 Scholar search

The search on scholar databases for technological innovations useful for the security and intelligence practitioners proved to be more appropriate and fruitful with respect to patent search, for this run of task T5.3.

Scholar authors often take opportunity in their work to highlight possible uses of the study’s subject by specific kinds of users, such as LEAs, and the filtering of results is more efficient, although not perfect.

Nevertheless, many of the keywords proposed in D5.1 for the breaking down of the focus areas lead to no results or too generic results. Thus, exploratory research was also performed on WP3 keywords (such as “OSINT”, “MASINT”, “IoT” etc.) and others, based on the expertise and attitude of the analysts.

The following issues were also encountered:

- the keyword “Intelligence” is almost always related to “Artificial Intelligence” rather than the Intelligence cycle;
- the keyword “Security” is almost always related to “health security” or “cyber security”;
- the keyword “SIGINT” leads to almost no results.

2.2 Research

2.2.1 Edge AI, biometric recognition, WST and IoT

This section reports about the search started with the keyword “MASINT”, which led to results about three technological families: Internet of Things (IoT), Edge Artificial Intelligence (Edge AI) and Biometric Recognition Technologies (BRTs).

The diagram below depicts how the research was developed:

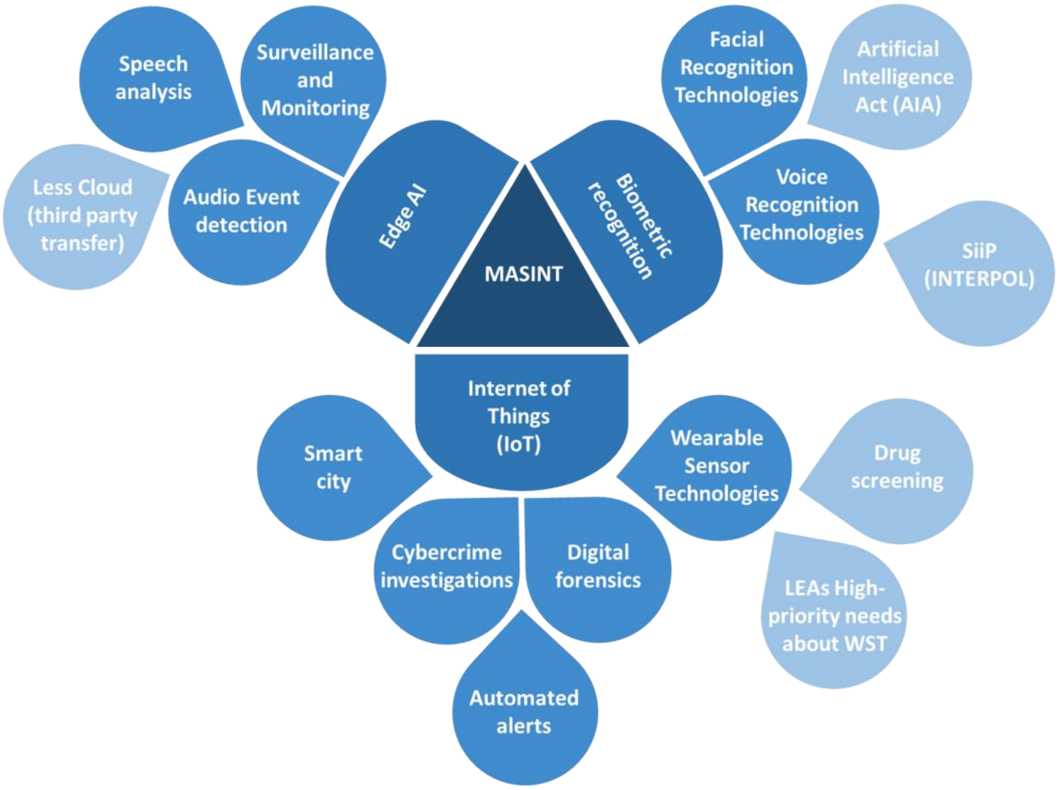

Speech analysis
Surveillance and Monitoring
Facial Recognition Technologies
Artificial Intelligence Act (AIA)
Less Cloud (third party transfer)
Audio Event detection
Edge AI
MASINT
Biometric recognition
Voice Recognition Technologies
SiiP (INTERPOL)
Internet of Things (IoT)
Smart city
Wearable Sensor Technologies
Drug screening
Cybercrime investigations
Digital forensics
LEAs High-priority needs about WST
Automated alerts

Figure 3: Diagram of the research about IoT, edge AI and BRTs

A search on the online scholar database *TheLens* with keyword "*MASINT*" in search fields abstract, title, keywords, and field of study with date range limitation to years 2019-2022 led to only 8 publications, no works cited by patents and no citing patents.

Despite the low number of publications retrieved, an interesting result was found about the application of Machine Learning on the edge to cyber-physical MASINT. The work is a Ph.D. thesis authored by David Elliot in 2020 at the Florida Institute of Technology and reports about efficient Edge Analytics applied to cyber-physical MASINT through machine learning on audio at the edge [5]. Elliot describes how, with the growth of the Internet of Things and the rise of Big Data, data processing and machine learning applications are being moved to cheap and low *size, weight, and power* (SWaP) devices at the edge, often in the form of mobile phones, embedded systems, or microcontrollers. The field of Cyber-Physical Measurements and Signature Intelligence (MASINT) makes use of these devices to analyse and exploit data in ways not otherwise possible, which results in increased data quality, increased security, and decreased bandwidth. However, methods to train and deploy models at the edge are limited, and models with sufficient accuracy are often too large for the edge device. Therefore, there is a clear need for techniques to create efficient AI/ML at the edge. The thesis presents training techniques for audio models in the field of environmental sound classification at the edge.

This result triggered additional research for possible applications of on the edge Artificial Intelligence for intelligence and security practitioners.

2.2.1.1 Edge AI

With the growth of Internet of Things (IoT) applications, billions of IoT devices are being connected to the Internet, generating massive amounts of data whose collection and processing in cloud data centres produces extremely high latency and network bandwidth usage. In this frame, **Edge AI** - the combination of edge computing and Artificial Intelligence to run machine learning tasks directly on connected edge devices - is the new frontier beyond the state of the art [6].

Edge Computing refers to computations being performed as close to data sources as possible instead of on external computing systems (the *Cloud*). Edge devices process the data of connected sensors that gather data: edge AI runs AI algorithms to process data directly on the hardware of the devices, providing rapid response times with low latency, high privacy, more robustness, and better efficient use of network bandwidth with respect to cloud computing.

This will enable AI in more appliances, connected products, healthcare wearables, etc., for fixed functions triggered locally by simple voice and gesture commands, common sounds, location and orientation, environmental conditions, vital signs, and so on [7].

Several applications appear to be promising for the field of security and intelligence [8]:

- *Surveillance and Monitoring:* Deep Learning-enabled smart cameras could locally process captured images to identify and track multiple objects and people, detecting suspicious activities directly on the edge node. These smart cameras minimise communication with the remote servers by only sending data on a triggering event, also reducing remote processing and memory requirements. Intruder monitoring for secure homes and monitoring of elderly people are typical applications.
- *Audio Event Detection*: Detecting sounds such as a baby crying, glass breaking, or a gunshot can trigger an action, including notifications or location detection, via triangulation. Since understanding specific sound events in multisource conditions is a latency-critical task, AI at the Edge can be very fast and effective recognizing an audio event among numerous overlapping sound sources.
- *Speech analysis:* Edge AI may also find application in the field of communication interception, with human speech analysis and understanding through Natural Language Processing (NLP) algorithms on the edge.

Edge AI may be further exploited for multimodal context analysis by receiving data from a variety of data sources and applying specific neural-network models to recognize more than just audio, video, or sensor data while simultaneously fusing all of it to better understand what is happening around the user, providing support to automate further actions.

Apart from the rapidness, low latency, high privacy and more robustness, the most interesting feature of edge AI solutions for security and intelligence practitioners appears to be the avoid of need to transfer data in the *Cloud*.

During the first workshop of NOTIONES (task T7.1) and the first working groups (task T6.1) the topic of transferring data used by LEAs in external servers, often in foreign nations, was recognised as a key issue. Edge AI may help solve this problem by significantly decrease the need of such data transfer, allowing to collect and process data locally, in real time.

2.2.1.2 Biometric Recognition Technologies

Analysts found some relevant results about edge-based tactical surveillance mobile application with facial recognition functionalities, which apparently has already proved to be useful for law enforcement and military police. For example, considering artificial intelligence-based tool triggering real-time alerts from a mobile device such as a bodycam or smartphone, providing threat intelligence to officers in one-on-one encounters or group situations, matching face biometrics against watch lists of dangerous or missing persons on the device (AnyVision, 2022). Further investigation on this theme triggered a new search about biometric recognition technologies and about smart devices (IoT) for LEAs.

A search on the online scholar database *TheLens* with keyword "*Biometric recognition*" and "*Law enforcement*" in search fields abstract, title, and full text with date range limitation to years 2020-2022 led to 112 publications, no works cited by patents and no citing patents.

Most of the search results led to legal/ethical issues. In this regard, a dedicated online search on the open web was performed about the attitude of EU institutions towards the use of biometric recognition technologies (see Annex I).

Apart from the ethical and legal issues, among the results of the scholar search another interesting publication emerged about the application biometric identity systems in law enforcement [9].

The paper reports about the results of the EU research Project SiiP (Speaker Identification Integrated Project) funded under the FP7 Programme with Grant Number 607784 between 2014 and 2018 [10]. SiiP is a European wide initiative to create the first international and interoperable database of voice biometrics, now the third largest biometric database at Interpol, which constitutes a particular 'regime of recognition' premised on the use of soft biometrics (age, language, accent and gender) to disembed voice in order to optimise for difference. This, in turn, has implications for the nature and scope of law enforcement, people's position in society, and justice concerns more broadly.

The project developed a solution based on a novel Speaker-Identification (SID) engine fusing multiple speech analytic algorithms (e.g. voiceprints recognition, Gender/Age/Language/Accent ID, Keyword/ Taxonomy spotting and Voice cloning detection), analysing rich metadata from voice samples and social media. It is used by INTERPOL [11] to detect individuals who use Internet-based applications (e.g. VoIP or social media) to plan a crime or terrorist attack, and provides judicial admissible evidence for identifying crime/terror suspects as well as for mapping/tracing the suspect terror/crime network. The data is stored in the SIIP Info Sharing Centre (SISC) located at INTERPOL.

Project	SiiP
Full Title	Speaker Identification Integrated Project
GRANT AGREEMENT ID:	607784
Source of information	https://cordis.europa.eu/project/id/607784
Topic	FP7-Security SEC-2013.5.1-2 - Audio and voice analysis, speaker identification for security applications – Integration Project
EU contribution	10 529 211 € out of 15 170 429,04 €
Coordinator	VERINT SYSTEMS Ltd (Israel)
Website:	https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP
Coordinator Contact:	Gideon Hazzani (Mr.) VERINT SYSTEMS Ltd Maskit Street 33 46733 Herzliya Israel
Funding Scheme	CP-IP - Large-scale integrating project
Start Date	1 May 2014
End Date	30 April 2018

2.2.1.3 Wearable Sensor Technologies

A search on the online scholar database *TheLens* with keyword “*IoT*” and “*Law enforcement*” in search fields abstract, title and full text on all years led to a thousand results, with a growing trend in recent years:

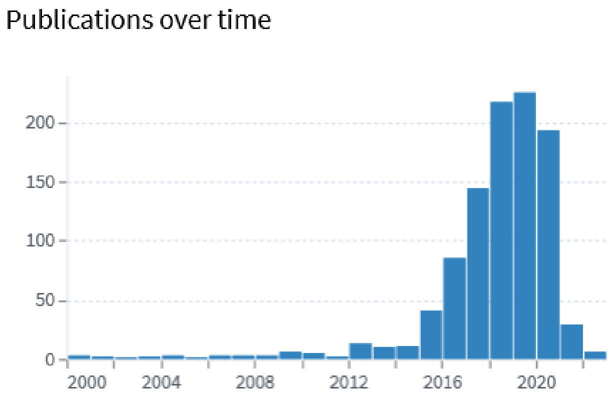


Figure 4: Statistical distribution of results for the search on the online scholar database TheLens with keyword “IoT” and “Law enforcement” in search fields abstract, title and full text in the date range 2000-2022

A more focused search on the online scholar database *TheLens* with keyword “*IoT*” and “*Law enforcement*” in search fields abstract, title, keywords and field of study with date range limitation to years 2020-2022 led to 110 publications, one work cited by patents and one citing patent.

A few publications were found about smart wearables. A paper by Teymourian et al. [12] reports about wearable electrochemical sensors capable of non-invasive monitoring of chemical markers, applied to the monitoring and screening of drugs in the health field. This may sound as something distant from NOTIONES, but the paper reports about the results of the EU research Project BorderSens (Border detection of illicit drugs and precursors by highly accurate electro sensors) funded under the H2020 Programme with Grant Number 833787 between 2019 and 2023 [13].

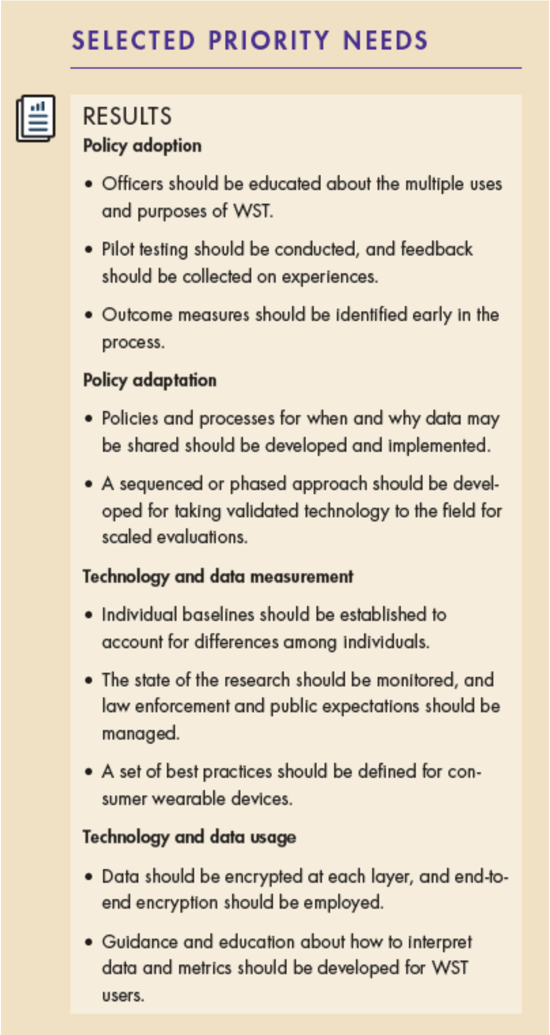
The main challenges posed by currently used on-site methods to detect illicit drugs and precursors are the low level of accuracy, in the case of colour tests, and the high costs and low portability, in the case of spectroscopic tests. In the light of a pressing need for better drug test systems at EU borders, the ultimate research aim of the BorderSens is to develop a portable, wireless single prototype device with the capability to quickly test for different types of drugs, precursors and adulterants/cutting agents, with outstanding accuracy and reduced false positives and false negatives. The project already has a very rich set of publications about illicit drug screening and monitoring [14] and may be deserve attention from the border guards and LEAs present in the NOTIONES network.

Project	BorderSens
Full Title	Border detection of illicit drugs and precursors by highly accurate electrosensors
GRANT AGREEMENT ID:	833787
Source of information	https://cordis.europa.eu/project/id/833787
Topic	H2020 SU-BES02-2018-2019-2020 - Technologies to enhance border and external security
EU contribution	€ 5 504 415
Coordinator	UNIVERSITEIT ANTWERPEN (Belgium)
Website:	https://bordersens.eu/
Coordinator Contact:	UNIVERSITEIT ANTWERPEN

	Prinsstraat 13 2000 Antwerpen Belgium
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Sep 2019
End Date	31 August 2023

Another work was found about wearable electrochemical sensors for rapid and on-site chemical threat assessment [15], dedicated in particular to first responders facing chemical and biological terror acts. The authors state that it is imperative that advances are made in bringing rapid chemical analysis directly into the field and that wearable electrochemical sensors are well placed to fill this technology gap to advance real-time chemical analytics at the point-of-need in diverse range of forensic, security and defence applications.

In the frame of Wearable Sensor Technology (WST), a very interesting 2020 report by RAND was found [16]. In this document, RAND reports about the outcomes of a 2019 workshop held at the offices of the Police Executive Research Forum in Washington D.C. to examine potential benefits of WSTs for improving individual officer safety, health, and wellness in law enforcement, examining the current and near-term state of portable WSTs, assess what opportunities can be realized using these devices and what potential pitfalls should be avoided. A summary of the results is provided below:



SELECTED PRIORITY NEEDS

RESULTS

Policy adoption

- Officers should be educated about the multiple uses and purposes of WST.
- Pilot testing should be conducted, and feedback should be collected on experiences.
- Outcome measures should be identified early in the process.

Policy adaptation

- Policies and processes for when and why data may be shared should be developed and implemented.
- A sequenced or phased approach should be developed for taking validated technology to the field for scaled evaluations.

Technology and data measurement

- Individual baselines should be established to account for differences among individuals.
- The state of the research should be monitored, and law enforcement and public expectations should be managed.
- A set of best practices should be defined for consumer wearable devices.

Technology and data usage

- Data should be encrypted at each layer, and end-to-end encryption should be employed.
- Guidance and education about how to interpret data and metrics should be developed for WST users.

Figure 5: Selected priority needs for WSTs in Law enforcement [16]

NOTIONES is called upon to carry out similar evaluations and analyses to security and intelligence practitioners, and this report may be used as a yardstick to assess differences with respect to the LEAs' perspective.

2.2.1.4 Internet of Things

Apart from WSTs, an interesting publication was also found about the legal challenges posed by IoT to cybercrime investigations and digital forensics [17]. The authors explore the challenges posed by cybercrime investigations and digital forensics concerning the shifting landscape of crime – the IoT and the evident investigative complexity – moving to the Internet of Anything (IoA)/Internet of Everything (IoE) era. IoT forensics requires a multi-faceted approach where evidence may be collected from a variety of sources such as sensor devices, communication devices, fridges, cars and drones, to smart swarms and intelligent buildings. Legal constraints and operational requirements should be discussed in order to enable the exploitation of such rich data valleys by security and intelligence practitioners.

Here, the multiple faces of IoT for security and intelligence applications emerge:

- on one side, IoT can be used by practitioners themselves to monitor threats in the field or individuals' health and safety, and for these applications there is a strong need for accuracy, reliability and security of the devices as well as of the data they collect, record and/or process.
- on the other hand, security and intelligence practitioners may need to monitor in real time the IoT devices of the individuals or organizations they are investigating – performing IoT data interception and hacking, exploiting security breaches in the devices;
- also, practitioners may need to retrieve data from such devices in order to collect evidence following a crime (digital forensics).

For the first point, initiatives are being held to promote trustworthy networks of things, focusing on network-centric approaches to improve the security and robustness of large-scale deployments of IoT devices [18] and developing protocols and best common practices that are directly relevant to the communication and security aspects of IoT [19]. This is an ongoing work, considering that security issues may arise at different layers of the IoT architecture, as depicted in the figure below:

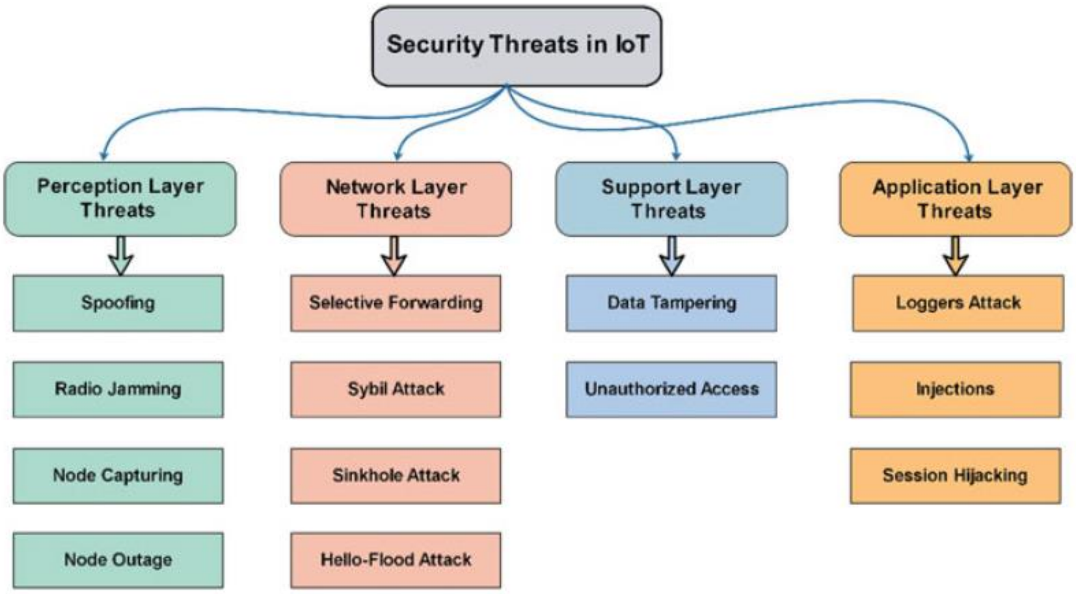


Figure 6: Security threats at different layers of the IoT architecture [20]

Practitioners should therefore assure the security of the IoT devices they are willing to use, while trying to breach the security of devices under investigation.

For the last point, authoritative papers [21] report a lack of a methodology and framework for IoT forensics, as well as a lack of appropriate tools for IoT forensics. A good overview of available forensics tools and their suitability for IoT was given in [22] in 2015, but existing traditional computer forensic tools were insufficient for cyber-crime investigations in IoT systems at the time. More recent publications propose dedicated IoT forensics solutions [20], but many challenges still remain.

2.2.2 Dark Net

This section deals with the use of “Dark Net” as a keyword searched on the online scholar database *TheLens* in search fields “abstract” and “title”.

The dataset was very heterogeneous, with results related to the fields of Physics (dark matter, dark energy, optics), Chemistry (photosynthesis), Computer Science (image enhancement). However, the analysts were able to extract several results related to Dark Net marketplace and Dark Web.

Intelligence directed towards the detection of illicit activities in the dark web social networks is described in a recent paper [23]. Here it is stated that many online chat applications are located in a grey area between the legitimate web and the dark net and that the Telegram network[6] in particular can be a platform for criminal activities. Classifying legitimate activity from illegitimate activity can help law enforcement agencies in finding criminals. To overcome the problem of users changing their username or creating new accounts to hide their identity, the authors explored classifying users from their language usage in their chat messages, using Machine Learning (ML) and Natural Language Processing (NLP) tools. It was found that legitimate and illegitimate chat groups could be classified with high accuracy, and it was also possible to classify bots, humans, and advertisements within conversations.

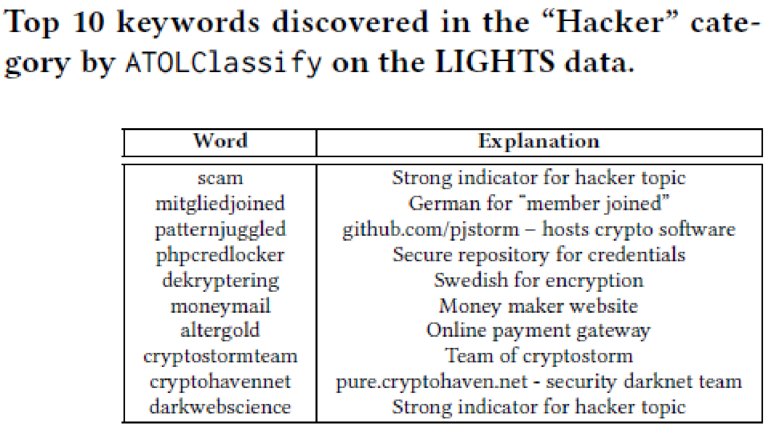
Another paper [24] introduces the game between the anonymous technologies underlying the Dark Web and the de-anonymization technologies and reports about the current status of data collection research in the dark web, analysing applications such as threat intelligence collection perception, underground economy investigation (with cryptocurrency tracking and tracing) and dark web/surface web association.

A particularly interesting work – for the purposes of NOTIONES – is a family of papers about the **categorisation of threats detected in the dark web**.

In 2017, Ghosh et al. published a paper about **ATOL** (Automated Tool for Onion Labelling) [25], an analytic component able to automatedly analyse and categorise the dark web ecosystem by learning descriptive and discriminative keywords for different categories, and then using them to describe the onion sites’ content. The code of the tool is openly available[7]. The tool operates on a repository of crawled onion sites and categorizes them based on keywords, i.e. the “weapons” category has keywords such as gun, Glock, silences, calibre etc. The initial keywords are analyst-provided, but the tool can also automatically discover new keywords associated to a certain category, as depicted in the figure below.

[6] https://web.telegram.org/k/

[7] http://www.csl.sri.com/users/vinod/atol/



Top 10 keywords discovered in the "Hacker" category by ATOLClassify on the LIGHTS data.

Word	Explanation
scam	Strong indicator for hacker topic
mitgliedjoined	German for "member joined"
patternjuggled	github.com/pjstorm – hosts crypto software
phpcredlocker	Secure repository for credentials
dekryptering	Swedish for encryption
moneymail	Money maker website
altergold	Online payment gateway
cryptostormteam	Team of cryptostorm
cryptohavennet	pure.cryptohaven.net - security darknet team
darkwebscience	Strong indicator for hacker topic

Figure 7: Example of ATOLClassify results source [25]

The tool is trained initially with labelled onion sites, and then with semi-supervised learning methods it is able to predict the category of a given unlabelled onion site with high accuracy.

As the authors state, the ATOL tool has several applications:

- Automated categorization of crawled sites;
- Extraction of keywords and persona attributes related to a certain category or theme;
- Generation of contextual metadata associated with a certain persona attribute.

The tool development was partially funded by the US National Science Foundation (NSF), the Defence Advanced Research Projects Agency (DARPA) under Air Force Research Laboratory and the Department of Homeland Security (DHS) Science and Technology Directorate.

The research in this field grew in the following years, as other works were published by the same authoring team until recent times [26] about the analysis of the darknet traffic for criminal activities detection. Other authors have obtained recently similar results [27], equating the accuracy of ATOL, but with a different approach to keywords: instead of using analyst-provided keywords, they extract keywords from legit documentation (i.e. law university libraries).

In this framework it should be reminded that DARPA developed a Dark Web crawler with advanced functionalities for fighting human trafficking, called MEMEX, back in 2014[8].

A systematic literature review of publications about dark web threat analysis can be found in [28], including scholar works about terrorism detection and Dark Net Markets (DNMs) monitoring for illicit trades.

With regard to applications of this kind of technology, information was found about major Dark Net investigations, such as the seize of big DNMs [29] [30]:

- Closure of DNM Silk Road (2013, FBI);
- Operation Commodore on DNM Utopia (2014, Dutch police);
- Operation Onymous on 11 DNMs (2014, FBI & Europol);
- Operation Bayonet on DNMs AlphaBay and Alpha (2017, FBI, DEA, Dutch police);
- Closure of DNM Wall Street Market (2019, German Public Prosecutor's office, Dutch Police, Europol, Eurojust, US agencies);

[8] https://memex.jpl.nasa.gov/index.html#page-top
https://www.darpa.mil/program/memex
https://www.youtube.com/watch?v=zDwoaZVFn50

- Closure of DNM Silkkitie (2019, Finish customs, French police, Europol);
- Closure of DNM DarkMarket (2021, international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom and the USA).

These are major, extensive operations. Intelligence and Security practitioners may be willing to perform more focused operations, for instance for the identification of a specific DNM vendor (selling explosives or weapons) or for tracing terrorist financing in the dark web.

3. Research monitoring on EU projects

This section reports the results of task T5.2, which performed a search on the European Community CORDIS (Community Research and Development Information Service) Platform[9] with regard to the most promising research projects in the field of intelligence and security.

Two steps of selection refinement were performed, preliminarily 37 and finally 12 promising projects were identified and investigated deeply.

3.1 Methodology

Following the indication of the deliverable D5.1 "*Methodology for Innovation Monitoring*", the activities of the task T5.2 have been focused on the deep survey of the most promising emerging technologies in the field of intelligence and security by highlighting the available results from EU research projects. To this purpose, the actual report is a tentative to rationalise and categorise knowledge exploited from the CORDIS database.

3.1.1 Data analysis techniques

The keyword-based retrieval of data from CORDIS and the desk research (research, evaluation and possible re-elaboration of information already collected by others, typically in textual format) were adopted as analysis techniques.

The preliminary dataset retrieval was obtained by searching on the CORDIS database the research projects mentioning keywords relevant to NOTIONES:

Table 1: Keywords used for the preliminary dataset retrieval

Key-words
intelligence security
security practitioners
terrorist threats
dark web
security research
horizon scanning
big data
mass surveillance
research monitoring
standardization needs
technologic solutions
supporting activities
European security
research programming
industry-academy
emerging technologies
artificial intelligence

The date range was set for projects starting from 2009. Such search resulted in a list of 71 interesting projects, which were investigated one by one in order to evaluate them on the base of alignment and interest of their objective and results with respect to the NOTIONES aims. After the evaluation, 37

[9] https://cordis.europa.eu

projects were selected out of the initial 71. These were further investigated by preparing info-tables and examining in deep the projects' objectives and results. Several of these projects were found to have interesting results in terms of available software or modelling, or in terms of relevance for the identified *focus areas*, and were further investigated. The selection process is depicted in the figure below.

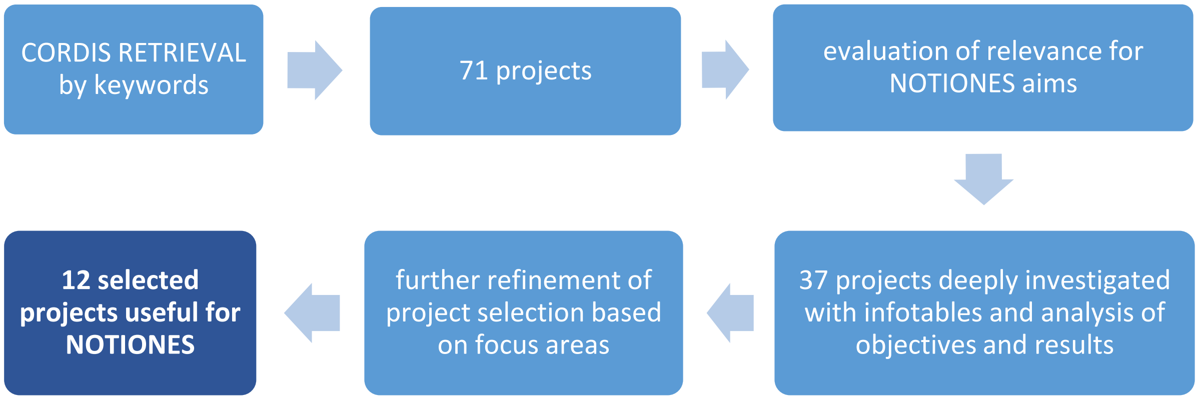

CORDIS RETRIEVAL by keywords
71 projects
evaluation of relevance for NOTIONES aims
37 projects deeply investigated with infotables and analysis of objectives and results
further refinement of project selection based on focus areas
12 selected projects useful for NOTIONES

Figure 8: T5.2 Process description

3.1.2 Profile of analyst(s)

The research was performed by Mr. Claudio Testani (Orcid ID: 0000-0002-5312-6016, Hi=13), who holds a Master's degree in Aerospace Structural Engineering (Univ. La Sapienza, Roma, Italy) and a PhD in Material Science (Univ. Tor Vergata, Roma, Italy). Moreover, holds the Italian ASN (qualification for Associate Professor) and he is member of the teaching board of the TorVergata University PhD School.

He is member of the European Enterprise Network sector group for Aeronautic, Defence and Aerospace and is member of the APRE - Cluster 4 (Industry, Digital and Space) Expert Team for Horizon Europe.

3.2 Research

As already described, 71 projects were initially retrieved from the CORID database. Of these, 37 projects survived the first selection refinement – see Annex II.

Between these 37, a total of 12 projects were found to have interesting results in terms of:

- relevance for the *Dark Web* focus area - (2 projects outlined);
- relevance for the *Data analysis phase of the intelligence cycle* focus area - (4 projects outlined);
- technology innovation (produced software or modelling) – (6 projects outlined).

A brief statistical analysis on the budget and participating countries of the original 71-projects dataset was also performed.

3.2.1 Selected projects for Dark Web

2 out of 37 projects were found to have interesting results in terms of relevance with the focus area *Dark Web*. The table below enlists these projects:

Table 2: Selected projects for Dark Web

acronym	title	start-end year
TITANIUM	Tools for the Investigation of Transactions in Underground Markets	2017-2020
DAN	High-performance, kiosk-solution for forensic darknet analysis to gain cyber threat intelligence for companies and greatly enhance efficiency and capabilities of European investigation authorities	2019-2020

Both projects were already listed in the NOTIONES Catalogue at the beginning of April 2022.

Below, the objectives and main results of these projects are reported.

3.2.1.1 TITANIUM

Project	TITANIUM
Full Title	Tools for the Investigation of Transactions in Underground Markets
GRANT AGREEMENT ID:	740558
Source of information	https://cordis.europa.eu/project/id/740558
EU contribution	€ 4 991 600
Coordinator	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Giefinggasse 4, 1210 Wien,
Website:	http://www.ait.ac.at/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999584128/740558
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 May 2017
End Date	30 Apr 2020

TITANIUM will develop novel methods and technical solutions for investigating and mitigating illegitimate activities (relating to either crime or terrorism) involving virtual currencies and/or underground market transactions. Specifically, the project will:

- Establish a research and development environment that enables close and continuous collaboration between researchers, developers, legal experts, and law enforcement stakeholders in several European countries and regions;
- Analyse legal and ethical requirements for tools and services, elicit technical requirements from LEA stakeholders, and establish a development ecosystem that ensures compliance with these requirements and supports the generation of court-proof evidence;
- Implement tools for the automated aggregation of data from diverse sources, including the dark web, the surface web, and other sources and devices obtained through legal warrants, using multi-modal adaptive crawlers, stealth facilities, and smart filters;
- Provide services for the simulation of criminal activities and the generation of synthetic data

- Investigate customizable heuristics, which can operate across different virtual currency transaction ledgers and identify clusters of addresses that are likely to belong to the same real-world entity;
- Apply novel techniques based on machine-learning and deep neural networks for revealing patterns, detecting anomalies, and identifying tumblers and mixers used for money laundering;
- Deploy forensics tools and services to partner LEAs and conduct Field Labs to assess the effectiveness, ethical and legal compliance, and overall impact of the results and to validate those results at technology readiness level (TRL) 6 or higher;
- Prepare curricula and carry out training and joint exercises that will facilitate the take-up of TITANIUM technologies by LEAs across Europe;
- Allow European SMEs and RTOs to develop cutting edge tools, to access LEA markets, and to strengthen European competitiveness.

3.2.1.2 DAN

Project	DAN
Full Title	High-performance, kiosk-solution for forensic darknet analysis to gain cyber threat intelligence for companies and greatly enhance efficiency and capabilities of European investigation authorities
GRANT AGREEMENT ID:	885845
Source of information	https://cordis.europa.eu/project/id/885845/results
EU contribution	50 000 Euro against 71 429 Euro
Coordinator	MH SERVICE GMBH Barthelsmuhlring 24, 76870 Kandel
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/911406569/885845
Funding Scheme	SME Inst Phase 1
Start Date	1 Oct 2019
End Date	31 Mar 2020

The dark web is often used by criminals as a platform for money laundering, purchasing weapons and dealing in sexual-related affairs, organs and illicit drugs trafficking and pornography. State institutions, banks and companies are most vulnerable to cyberattacks originating in the dark web. Due to its covert nature, it’s difficult for police to investigate. In addition, companies are seeking reliable and effective ways to protect their data from groups working in the dark web. The EU-funded DAN project proposes a solution that consists of high-performance hardware, pre-installed and pre-configured intuitive software. It also provides training and seminars to the users. The solution isolates and protects from any foreign interference or access the acquired data and secures the chain of evidence for investigation and privacy for companies.

The Dark Web is an ideal virtual space for criminals. It has become a forum and marketplace for weapons, drugs, organs, illicit pornography, software exploits, stolen private data, passwords, credit card details, counterfeit products and money. Illegal services are offered, like phishing, cyber-attacks, murder and rape for hire and money laundering.

Criminal investigation authorities began to investigate cases of crimes and terrorism in the Dark Web, but struggle to access, handle and analyse the immense amount of data, and urgently need an isolated solution to acquire solid evidence legally applicable in court. For corporations, the potential economic and image damage of cyber-attacks is extensive. They search adequate solutions to acquire cyber threat intelligence, to identify threats, enhance cyber defence and allow a fast and effective response. Up to now, commercial state-of-the-art solutions force users to into third party services or to access crawled data on online clouds.

mh SERVICE, Europe’s leading provider and supplier of products and services related to IT forensics and consortium leader of the project, developed DAN, a Kiosk solution for darknet analysis. It includes high-performance hardware, pre-installed and pre-configured intuitive software, as well as user training and seminars. The acquired data is isolated from the possibility of foreign access or manipulation by third persons to ensure the chain of evidence for investigation authorities and privacy for companies. During the feasibility study of DAN, the prototype was tested at several customers and now optimise and redesign the DAN to perfectly fulfil the user needs from both segments.

3.2.2 Selected projects for Intelligence

4 out of 37 projects were found to have interesting results in terms of relevance with the focus area *Data Intelligence phase in the Intelligence cycle*. The table below enlists these projects:

Table 3: Selected projects for Intelligence

acronym	title	start-end year
PREVISION	Prediction and Visual Intelligence for Security Information	2019-2021
INFINITY	IMMERSE. INTERACT. INVESTIGATE	2020-2023
TRACE	Tracking illicit money flows	2021-2024
CYBER-TRUST	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things	2018-2021

All projects were already listed in the NOTIONES Catalogue at the beginning of April 2022.

Below, the objectives and main results of these projects are reported.

3.2.2.1 PREVISION

Project	PREVISION
Full Title	Prediction and Visual Intelligence for Security Information
GRANT AGREEMENT ID:	833115
Source of information	SU-FCT03-2018-2019-2020 - Information and data stream management to fight against (cyber)crime and terrorism
Call for Proposal	H2020-SU-SEC-2018
EU contribution	€ 9 040 230,00
Coordinator	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS Patission Str. 42 10682 Athina Greece
Website:	https://www.iccs.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999654356/833115
Funding Scheme	IA - Innovation action
Start Date	01/09/2019
End Date	31/12/2021

The EU-funded PREVISION project will provide law enforcement agencies with advanced, almost-real-time, analytical support for multiple Big Data streams (coming from various data sources). The project will allow for building dynamic and self-learning knowledge graphs that will help investigators become more aware in these fields and better address hybrid security threats, i.e. threats that combine physical and cyber-attacks. The project will organise five representative and complementary use cases, including the protection of public spaces and the fight of illicit trafficking of antiquities, in full compliance with privacy requirements, human rights and applicable law.

The mission of PREVISION is to empower the analysts and investigators of LEAs with tools and solutions not commercially available today, to handle and capitalise on the massive heterogeneous data streams that must be processed during complex crime investigations and threat risk assessments. With criminals being ever more determined to use new and advanced technology for their purposes, the aim is to establish PREVISION as an open and future-proof platform for providing cutting-edge practical support to LEAs in their fight against terrorism, organised crime and cybercrime, which represent three major cross-border security challenges that are often interlinked. PREVISION provides advanced near-real-time analytical support for multiple big data streams (coming from online social networks, the open web, the Darknet, CCTV and video surveillance systems, traffic and financial data sources, and many more), subsequently allowing their semantic integration into dynamic and self-learning knowledge graphs that capture the structure, interrelations and trends of terrorist groups and individuals, cybercriminal organisations and organised crime groups, giving rise to enhanced situational awareness in these fields.

PREVISION has a pan-European engagement and support agenda for LEAs: ten (10) different LEAs and practitioners take part in its consortium, while additional ones (including Europol) have joined its external advisory board. A strong inter-disciplinary dimension, combining technological expertise with sociological, psychological, linguistic and data science models, will lead to a common strategic approach for predicting abnormal and deviant behaviour, radicalisation potential, threat risks for soft targets, and cybercrime trends at different timescales. PREVISION will conduct demonstrations on five representative and complementary use cases, under real-life operational conditions, in full compliance with fundamental rights and applicable legislation.

3.2.2.2 INFINITY

Project	INFINITY
Full Title	IMMERSE. INTERACT. INVESTIGATE
GRANT AGREEMENT ID:	883293
Source of information	https://cordis.europa.eu/project/id/883293
EU contribution	€ 6 866 503,75
Coordinator	AIRBUS DEFENCE AND SPACE SAS 31 Rue Des Cosmonautes Zi Du Palays 31402 Toulouse Cedex
Website:	http://www.astrium.eads.net/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999809265/883293
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 June 2020
End Date	31 May 2023

The EU-funded INFINITY project will couple virtual and augmented reality innovations, artificial intelligence and machine learning with big data and visual analytics. Its aim will be to deliver an integrated solution to revolutionise data-driven investigations. The project will address the core needs of contemporary law enforcement by equipping investigators with cutting-edge tools to acquire, process, visualise and act upon the enormous quantities of data they are faced with every day. It will assist law enforcement agencies with automated systems and instinctive interfaces and controls.

Infinity's ambition is to become a flagship project against society's most pressing cybercriminal, terrorist and hybrid threats. Synthesising the latest innovations in virtual and augmented reality, artificial intelligence and machine learning with big data and visual analytics, Infinity will deliver an integrated solution that aims to revolutionise data-driven investigations. Bringing together a strong representation from national and supranational agencies with an end-user-driven design, it will directly address the core needs of contemporary law enforcement. Specifically, it will equip investigators and analysts with cutting-edge tools to acquire, process, visualise and act upon the enormous quantities of data they are faced with every day. Bolstered by cognitive research, automated systems and instinctive interfaces and controls, Infinity will be designed and developed to maximise the potential of individual investigators. On a collective level, the immersive collaborative environment offered by Infinity will enable co-located and remote LEA cooperation in ways that have not yet been realised. This end-to-end system for LEA operations will cover the full investigative cycle, including generating reports for decision-makers and admissible evidence to demonstrate to juries and judges. Ultimately, the solutions offered by Infinity will propel LEAs ahead of traditional and evolving complex, hybrid and transnational threats and protect the societies they serve.

3.2.2.3 TRACE

Project	TRACE
Full Title	Tracking illicit money flows
GRANT AGREEMENT ID:	101022004

Source of information	https://cordis.europa.eu/project/id/101022004
EU contribution	€ 963 875,00
Coordinator	COVENTRY UNIVERSITY Priory Street, CV1 5FB Coventry UK
Website:	http://www.coventry.ac.uk/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999612161/101022004
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 July 2021
End Date	30 June 2024

The EU-funded TRACE project will explore the rise and spread of ICT-enabled crimes and illicit financial flows (IFFs). Considering that innovative policing tools are required to patrol the virtual routes, the project will focus on new ways to identify, track and document IFFs. In consultation with law enforcement agencies, the project will apply its solutions in use cases on terrorist financing, web forensics, cyber extortion and use of cryptocurrencies in money laundering in arts and antiquities, and online gambling. It will also set up a working group of law enforcement agencies and other stakeholders to discuss good practices in information sharing.

With the rise and spread of ICT-enabled crimes and illicit financial flows (IFFs), law enforcement agencies (LEAs) and financial intelligence units (FIUs) need innovative policing tools in the virtual sphere as well as skills, organisational and regulatory adaptations to counter these threats. TRACE will focus on input (forming initial suspicion), processing (substantiating suspicion, collecting evidence, locating suspects and their assets) and output (producing court proof / admissible e-evidence) to develop ICT-enabled solutions to identify, track and document IFFs, to pave the way for recovering the proceeds of crime and to disrupt the IFFs. TRACE will apply its solutions in use cases on terrorist financing, web forensics, cyber extortion, use of cryptocurrencies in property market transactions, money laundering in arts and antiquities, and online gambling, all of which have been developed in consultation with LEAs. TRACE will make recommendations on harmonisation of information formats in suspicious activity reports. Heretofore the differences and fragmented use of e-evidence in criminal justice processes have hindered cross-border investigations, prosecutions and convictions and recovery of assets. TRACE will create an open source platform for LEAs and for advancements in technology-based solutions in policing. With stakeholder engagement from the outset, the TRACE partners will co-develop advanced investigation tools and test and validate their efficacy in detecting IFFs. TRACE will also create a working group of partner LEAs and Stakeholder Board LEAs to discuss good practices in information sharing among EU LEAs. The project will create a Stakeholder Board of about 20 key stakeholders and an Ethics Advisory Board comprising four external ethics experts and two partners. TRACE has a multidisciplinary consortium comprising LEAs, AI technology companies, academia, research institutes and NGOs with track records of delivering cutting edge EU projects.

3.2.2.4 CYBER-TRUST

Project	CYBER-TRUST
Full Title	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
GRANT AGREEMENT ID:	786698
Source of information	https://cordis.europa.eu/project/id/786698
EU contribution	€ 2 996 182,50
Coordinator	KENTRO MELETON ASFALEIAS, P Kanellopoulou 4 St 10177 Athina, Gr

Website:	https://ec.europa.eu/research/participants/documents/ downloadPublic?documentIds=080166e5bd8ccc07&appId=PPGMS
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999827307/786698
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 May2018
End Date	31 July 2021

The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform to tackle the grand challenges towards securing the ecosystem of IoT devices. The security problems arising from the flawed design of legacy hardware and embedded devices allows cyber-criminals to easily compromise them and launch large-scale attacks toward critical cyber-infrastructures. The proposed interdisciplinary approach will capture different phases of such emerging attacks, before and after known (even years old) or unknown (zero-day) vulnerabilities have been widely exploited by cyber-criminals to launch the attack. Emphasis is given on building a proactive cyber-threat intelligence gathering and sharing system to prevent the exploitation of zero-day vulnerabilities. This intelligence information will be used to maintain accurate vulnerability profiles of IoT devices, in accordance with data protection, privacy, or other regulations, and optimally alter their attack surface to minimise the damage from cyber-attacks. Novel technologies will be developed, based on distributed ledgers and blockchains, to monitor devices' integrity state and network behaviour that will considerably increase the detection and response capabilities against targeted and interdisciplinary cyber-attacks. In the case of alleged malicious activity, tools for collecting and storing forensic evidence on a tamper-proof blockchain structure will be delivered, taking into account the specific needs of law enforcement agencies. Privacy-preserving network monitoring and advanced virtual reality-based visualisation techniques will be employed for quickly detecting botnets, DDoS attacks and other incidents. Relying on interdisciplinary research, an intelligent autonomous cyber-defence framework will be built for providing intelligent ways of isolating the devices under an attacker's control (or infected) and effectively responding to and mitigating large-scale attacks.

3.2.3 Selected projects for technology innovation

6 out of 37 projects were found to have interesting results in terms of available software or modelling, and were further investigated in a deeper way. The table below enlists these projects:

Table 4: Selected projects for technology innovation

acronym	title	start-end year	type of result
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion	2019-2022	Software via OpenAIRE
ECHO	European network of Cybersecurity centres and competence HUB for Innovation and Operations	2019-2023	ECHO Web Platform
COSMIC	CBRNE Detection in Containers	2018-2021	Guideline and Reports
CONNEXIONs	InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services	2018-2022	Software via OpenAIRE

acronym	title	start-end year	type of result
ADABTS	Automatic Detection of abnormal Behaviour and Threats in crowded Spaces	2009-2013	Generative models for pedestrian track analysis
INSIKT	Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization	2017-2020	Software via OpenAir (INVISO Platform)

Of these, only CONNEXIONs was listed in the NOTIONES Catalogue at the beginning of April 2022.

Below, the objectives and main results of these projects are reported.

3.2.3.1 CONCORDIA

Project	CONCORDIA
Full Title	Cyber security cOmpeteNCe fOr Research anD InnovAtion
GRANT AGREEMENT ID:	830927
Source of information	https://cordis.europa.eu/project/id/830927
EU contribution	€ 15 998 737,50
Coordinator	UNIVERSITAET DER BUNDESWEHR MUENCHEN Werner Heisenberg Weg 39, 85579 Neubiberg
Website:	http://www.unibw.de/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999630009/830927
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Jan 2019
End Date	31 Dec 2022

Europe has incredible coverage and talent in the area of IT and cybersecurity, but the area of cybersecurity is geographically fragmented across Europe for competences, and often also technically fragmented with problem-specific development of security solutions.

CONCORDIA addresses the EU's strategic interest to develop and hold on to its security capacities by mitigating its current fragmentation through the interconnection of Europe's cybersecurity capabilities into a network of expertise to help build a secure, trusted, resilient and competitive ecosystem.

The CONCORDIA network includes forces across Europe's research, industry and public sector and to include all talents not just those that have representation in the EU mainstream or are within big organizations. CONCORDIA addresses the current fragmentation of security competence by networking diverse competences into a leadership role via a synergistic agglomeration of a pan-European Cybersecurity Centre.

Technologically, CONCORDIA projects a broad and evolvable data-driven and cognitive E2E Security approach for the ever-complex ever-interconnected compositions of emergent data-driven cloud, IoT and edge-assisted ICT ecosystems.

Software via OpenAIRE (3)	OpenAIRE
HTTPS Event-Flow Correlation Improving Situational Awareness in Encrypted Web Traffic - Data and Code https://doi.org/10.5281/zenodo.5821815	" **Author(s):** Špaček, Stanislav; Velan, Petr; Čeleda, Pavel; Tovarňák, Daniel **DOI:** oai:zenodo.org:5821815; 10.5281/zenodo.5821815 **Publisher:** Zenodo
Software for: "It is just a flu: Assessing the Effect of Watch History on YouTube's Pseudoscientific Video Recommendations" https://doi.org/10.5281/zenodo.4580891	**Author(s):** Papadamou, Kostantinos; Zannettou, Savvas; Blackburn, Jeremy; De Cristofaro, Emiliano; Stringhini, Gianluca; Sirivianos, Michael **DOI:** 10.5281/zenodo.4580999; 10.5281/zenodo.4580892; 10.5281/zenodo.4580891 **Publisher:** Zenodo
Software for "Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls" https://doi.org/10.5281/zenodo.2563838	**Author(s):** Zannettou, Savvas; Caulfield, Tristan; Setzer, William; Sirivianos, Michael; Stringhini, Gianluca; Blackburn, Jeremy **DOI:** 10.5281/zenodo.2563839; 10.5281/zenodo.2563838 **Publisher:** Zenodo

3.2.3.2 ECHO

Project	ECHO
Full Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
GRANT AGREEMENT ID:	830943
Source of information	https://cordis.europa.eu/project/id/830943
EU contribution	€ 15 987 285
Coordinator	ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL Avenue De La Renaissance 30, 1000 Bruxelles
Website:	https://echonetwork.eu/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999831575/830943
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Feb 2019
End Date	31 Jan 2023
Comments	NOTIONES partner Z&P is in the consortium

The project ECHO aims to deliver an organised and coordinated approach to improve proactive cyber defence of the European Union, allowing the bloc to act in anticipation, defending against an attack on computers and networks. ECHO is developing a network through which the EU's Cybersecurity and Competence Centres can be best coordinated and optimised. This can help contribute to a lasting and sustainable development of cybersecurity skills, including increased research and experimentation for certified security products such as early warning systems and inter-sector technology roadmaps.

ECHO will model and demonstrate a network of cyber research and competence centres, with a central competence at the hub. The Central Competence Hub serves as the focal point for the ECHO Multi-sector Assessment Framework enabling multi-sector dependencies management, provision of an Early Warning System, a Federation of Cyber Ranges and management of an expanding collection of Partner Engagements.

The ECHO Cyber-skills Framework will also provide the foundation for development of cybersecurity education and training programmes including a common definition of transversal and inter-sector skills and qualifications needed by cybersecurity practitioners.

ECHO is one of the four pilot projects financed under Horizon 2020 aiming to connect and share knowledge across multiple domains, representing the building framework of the European Cybersecurity Competence Centre located in Bucharest.

3.2.3.3 COSMIC

Project	COSMIC
Full Title	CBRNE Detection in Containers
GRANT AGREEMENT ID:	786945
Source of information	https://cordis.europa.eu/project/id/786945
EU contribution	€ 3 498 867,50
Coordinator	LINGACOM LTD 10 Hanechoshet Street Ramat Hachayal, 69710 Tel Aviv
Website:	https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c2e7310a&appId=PPGMS
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/937796971/786945
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Oct 2018
End Date	30 Sep 2021

The threat of CBRNE (Chemical, Biological, Radiological, Nuclear and Explosives) components used by terrorists is a major concern for EU and worldwide security and there is a gap in the existing security flow that can be used by terrorists to hide and smuggle CBRNE materials inside containers and vehicles. Improvised Nuclear Device (IND) could be detonated using nuclear weapon components, modified nuclear weapons, or a self-made device and Radiological Dispersal Device (RDD) could be designed to disperse radioactive materials through an explosion (or 'dirty bomb').

COSMIC addresses the challenge of improving container and vehicles border crossing and critical infrastructure entrance security checks, bridging the major security gap for fast inspection of large number of containers and vehicles in seaport and in crossing borders for CBRNE materials. COSMIC's technology can be adapted also to air containers.

COSMIC proposes a novel technological approach for the detection of CBRNE materials hidden in shipping containers. COSMIC project includes the research, design and implementation of a three stage (primary, secondary, focused manual inspection) detection system using new set of innovative sensors.

Main Results:

1	SoA and Guideline for Technology[10]	REPORT
2	Report on Standardisation activities[11]	REPORT
3	Report on Scientific Papers and Dissemination[12]	REPORT
4	Report on Training[13]	REPORT

3.2.3.4 CONNEXIONs

Project	CONNEXIONs
Full Title	InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services
GRANT AGREEMENT ID:	786731
Source of information	https://cordis.europa.eu/project/id/786731 https://www.connexions-project.eu/
EU contribution	€ 4 999 390
Coordinator	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS, Charilaou Thermi Road 6 Km, 57001 Thermi Thessaloniki, Greece
Website:	http://www.certh.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/998802502/786731
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 September 2018
End Date	28 Feb 2022

CONNEXIONs aims to develop and demonstrate next-generation detection, prediction, prevention, and investigation services. These services will be based on multidimensional integration and correlation of heterogeneous multimodal data, and delivery of pertinent information to various stakeholders in an interactive manner tailored to their needs, through augmented and virtual reality environments.

The CONNEXIONs solution encompasses the entire lifecycle of law enforcement operations including:

a) pre-occurrence crime prediction and prevention;

b) during-occurrence LEA operations;

c) post-occurrence investigation, and crime-scene simulation and 3D reconstruction.

CONNEXIONs will meaningfully enhance operational and (near) real-time situational awareness, through automated identification, interpretation, fusion and correlation of multiple heterogeneous big data sources, as well as their delivery via immersive solutions. Such multimodal data include Surface/Deep/Dark Web and social media content in 7 languages (EN, FR, DE, PT, RO, ES, AR), data acquired by Internet of Things (IoT) devices, and digital evidence. CONNEXIONs will also provide chain-of-custody and path-to-court for digital evidence.

CONNEXIONs will be validated in field tests and demonstrations in 3 operational use cases:

a) counter-terrorism security in large scale public events

[10] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c1f6fdfd&appId=PPGMS

[11] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df180b67&appId=PPGMS

[12] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e2afda91&appId=PPGMS

[13] Report on Training

b) human trafficking investigations and mitigation

c) crime investigation and training through 3D scene reconstruction

Extensive training of LEAs' personnel, hands-on experience, joint exercises, and training material will boost the uptake of CONNEXIONs tools and technologies.

Main Result:

Software via OpenAIRE	SOFTWARE
	First demonstrator of creation of BIM and GIS models for optimal surveillance &amp; 3D scene reconstruction. **Author(s):** Nikolaos Patsiouras; Xenophon Zabulis **DOI:** 10.5281/zenodo.4432099; 10.5281/zenodo.4432100 **Publisher:** Zenodo

3.2.3.5 ADABTS

Project	ADABTS
Full Title	Automatic Detection of abnormal Behaviour and Threats in crowded Spaces
GRANT AGREEMENT ID:	218197
Source of information	https://cordis.europa.eu/project/id/218197/reporting
EU contribution	€ 3 229 034 of a total costs : € 4 523 994
Coordinator	TOTALFORSVARETS FORSKNINGSINSTITUT,
Website:	http://www.foi.se/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999627875/218197
Funding Scheme	CP - Collaborative project (generic)
Start Date	1 Aug 2009
End Date	30 July 2013

ADABTS aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime, and riots, by the automatic detection of abnormal human behaviour.

Current automatic detection systems have limited functionality, struggling to make inferences about the acceptability of human behaviour. ADABTS aims to address one of the key problems, the definition of abnormal behaviour, by extracting characterizations in realistic security settings based on expert classifications and the analysis of CCTV operator behaviour.

A set of behaviour descriptors will be defined and models of threatening behaviour will be built. Algorithms will be developed that detect pre-defined threat behaviours and deviations from normal behaviour. For accurate and robust detection, data from audio and video sensors will be combined with context information. The trade-off between system generality and capability is addressed by extracting a set of intermediate-level behaviour descriptors that are observable from sensor data. This makes the system configurable to specific needs and improves scalability and cost efficiency.

A real-time evaluation platform will be developed based on commercial heterogeneous hardware. Such hardware, in rapid development driven by the video game industry, represents a huge potential for high-performance low-cost surveillance systems. The evaluation platform will demonstrate pro-active detection of potential threats. The context will be large-scale events, represented by a football arena, and critical infrastructure, represented by international airports.

The involvement of stakeholders (security system operators and integrators, police organizations, airports, event organizers) will ensure relevance and exploitation.

Publications via OpenAIRE (1)	OpenAIRE
Generative models for pedestrian track analysis: https://dare.uva.nl/personal/pure/en/publications/generative-models-for-pedestrian-track-analysis(0987b174-5b10-4c7f-be13-27d824e213ed).html	**Author(s):** Kooij, J.F.P. **Permanent ID:** Handle:11245/1.506702

3.2.3.6 INSIKT

Project	INSIKT
Full Title	Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization
GRANT AGREEMENT ID:	767542
Source of information	https://cordis.europa.eu/project/id/767542
EU contribution	€ 1 533 153,13 against a total costs of: € 2 190 218,75
Coordinator	INSIKT INTELLIGENCE S.L Calle Huelva 106, 9-4 08020 Barcelona, ES
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/919371045/767542
Funding Scheme	
Start Date	1 Oct 2017
End Date	30 Mar 2020

In 2015-2016, more than twenty terrorist attacks occurred in EU28, all of them carried out by individuals radicalized by terrorist propaganda. Recruitment of this new breed of terrorists was done via social media and the Internet. To prevent such events from happening in the future and fight radicalization, it is crucial to detect cyber-propaganda early. However, social media providers (e.g. Twitter) admit that at the moment there is no adequate tool to identify terrorist-related content on the Internet. As the result, they are forced to rely on proprietary spam-fighting tools, user reports and human analysis to track down radicalized accounts that promote terrorism.

The Consortium leader of INSIKT is Insikt Intelligence, a Spanish SME that developed a novel social data mining platform to detect & defeat violent online radicalization. An early version of INSIKT platform was validated by several EU law enforcement agencies (LEAs), approved and attracted commercial interest. INSIKT provides a novel solution for LEA analysts to detect terrorist propaganda on all social media: it identifies radical content, suspicious messages and covert radicalization process with the help of sophisticated text mining algorithms. INSIKT relies on deep learning to develop automatically new models which can be used to detect other criminal activity as well. INSIKT is fit to become an important new tool in LEAs' investigation and evidence gathering arsenal, giving them highly accurate, multilingual and real-time detection capabilities.

Main result: INVISO, a SOCMINT solution

In this context, LEAs are looking at social media intelligence (SOCMINT) as the potential solution to this growing problem. By combining natural language processing with social network analysis and artificial intelligence, SOCMINT tools could be just what they need to fight online radicalisation. INVISO[14] is one of these tools. It stands out with its unique user interface, user experience and, of course, the tech behind it. In the words of the INSIKT Intelligence CEO: "*INVISO identifies radical content, suspicious messages and covert radicalisation processes with the help of sophisticated text mining algorithms. The platform also relies on deep learning to automatically develop new models which can be used to detect other criminal activities. It really stands out from a technical perspective, as only a handful of competing technologies are LEA-specific and most of them lack automated detection capabilities and artificial intelligence. They do not learn from users' input like INVISO does, preventing them from increasing accuracy over time or learning from past cases*."

To devise INVISO, INSIKT Intelligence has been working closely with LEAs. Experts from the International Institute for Counter-Terrorism have notably shared their insights as development moved forward, enabling the INSIKT team to develop a model for the detection of pre-radicalisation. In other words, INVISO not only detects threatening posts, it also analyses overall online behaviour and provides a probability of a user becoming radicalised. INVISO is expected to completely change the way LEA investigators work. In the words of the INSIKT Intelligence CEO: "*They can automate a large part of their intelligence gathering tasks with the system and concentrate on other important work. Once launched, we will be looking to commercialise the product all over Europe. But it should be noted that INVISO will keep evolving after that. We will continuously be updating the platform and adding new ground breaking tools to keep up with technological advancements. We want to ensure that LEAs are fully equipped to combat online crime and prevent the spread of radical content*".

3.2.4 Statistical analysis on budget and nationality

The original dataset of 71 projects was subject to statistical analysis with regard to budgeting and Countries involved. The results are synthesized in **¡Error! No se encuentra el origen de la referencia.**:

Table 5: Statistical analysis: budget and Countries

Country	Funding Budget received	Number of Projects with at least one partner from the Country	Total number of partners from the Country in the proejcts	Number of projects in which the coordinator is from the Country
Germany	52.399.000 €	49	117	14
UK	25.369.000 €	42	65	12
Greece	29.903.000 €	37	80	12

[14] http://www.insiktintelligence.com/our-solutions/inviso-intelligence-platform/

Country	Funding Budget received	Number of Projects with at least one partner from the Country	Total number of partners from the Country in the proejcts	Number of projects in which the coordinator is from the Country
Spain	31.759.000 €	41	93	9
France	49.401.000 €	43	101	6
Sweden	12.697.000 €	18	23	5
Finland	11.519.000 €	18	29	3
Belgium	21.121.000 €	29	53	3
Italy	36.624.000 €	39	105	2
Netherlands	27.954.000 €	37	73	2
Bulgaria	6.308.000 €	9	23	1
Israel	5.243.000 €	8	12	1
Denmark	1.412.000 €	6	5	1
Austria	17.381.000 €	22	38	1
Portugal	6.523.000 €	21	29	1
Hungary	2.736.000 €	6	9	1
Luxemburg	2.313.000 €	6	7	1
Estonia	5.161.000 €	11	15	0
Poland	6.817.000 €	14	24	0
Latvia	439.000 €	2	3	0
Bosnia & Herzegovina	20.000 €	1	1	0
Slovakia	779.000 €	6	9	0
Ukraine	347.000 €	3	3	0
Georgia	43.000 €	1	1	0
North Macedonia	134.000 €	2	2	0
Ireland	5.124.000 €	11	15	0
Norway	5.911.000 €	9	19	0
Lithuania	1.203.000 €	4	5	0
Romania	4.907.000 €	17	31	0
Cyprus	3.216.000 €	10	14	0
Czechia	3.198.000 €	11	13	0
Croatia	518.000 €	5	5	0
Tunisia	459.000 €	2	2	0
Moldova	141.000 €	2	2	0
Switzerland	4.114.000 €	12	17	0
Slovenia	1.569.000 €	6	11	0

Country	Funding Budget received	Number of Projects with at least one partner from the Country	Total number of partners from the Country in the proejcts	Number of projects in which the coordinator is from the Country
Turkey	977.000 €	2	6	0
Malta	787.000 €	2	3	0
USA	603.000 €	2	3	0
Serbia	202.000 €	2	3	0
China (*)	613.000 €	1	8	0

(*) Budget allocated for activities is not the budget funded by EU

Germany is the Country that is more active with 117 Partnerships and 14 Coordination of Projects.

Germany, UK, Greece, Spain, France and Sweden are the Top 5 Countries in the Sector according the number of Projects activated and funded by the European Community.

A further analysis step is related to the budget (Figure 9):

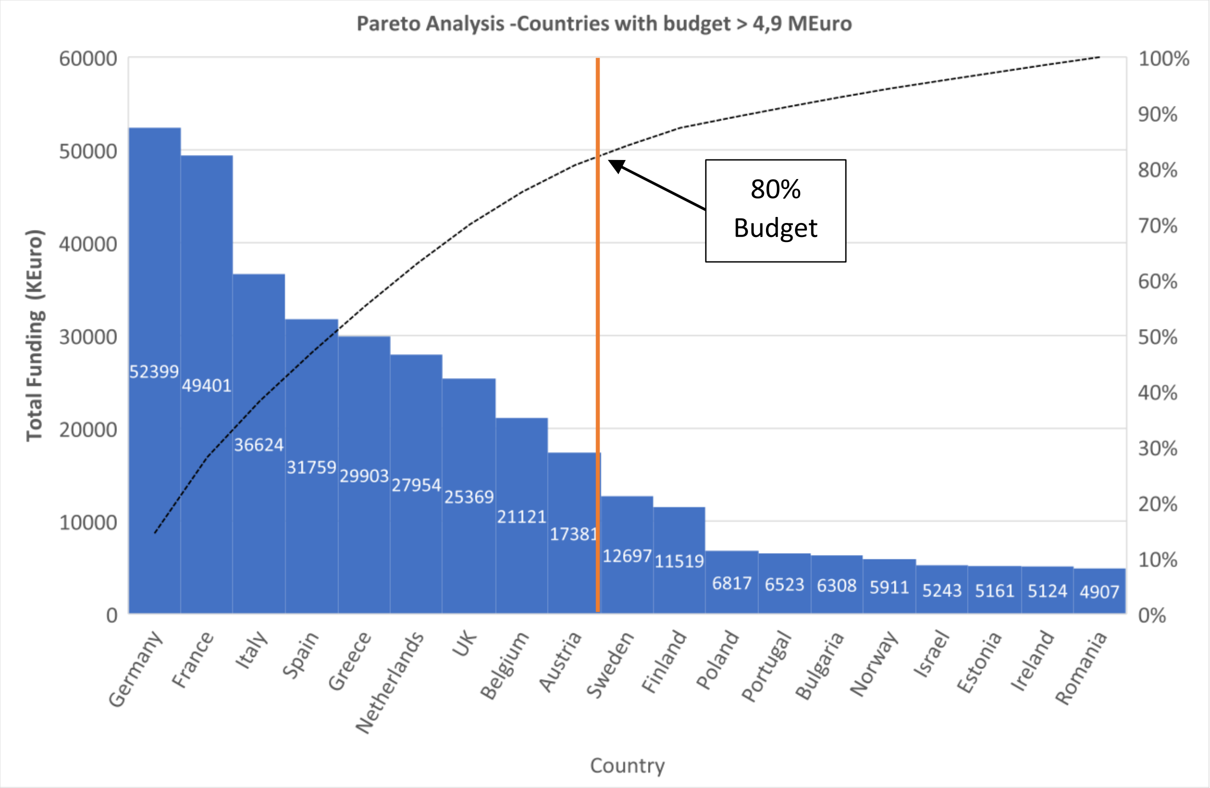


Figure 9: Pareto Graph for the budget distribution among Countries

The Pareto graph permits to conclude that the 60% of the total budget is covered by only 5 Countries: Germany, France, Italy, Spain and Greece.

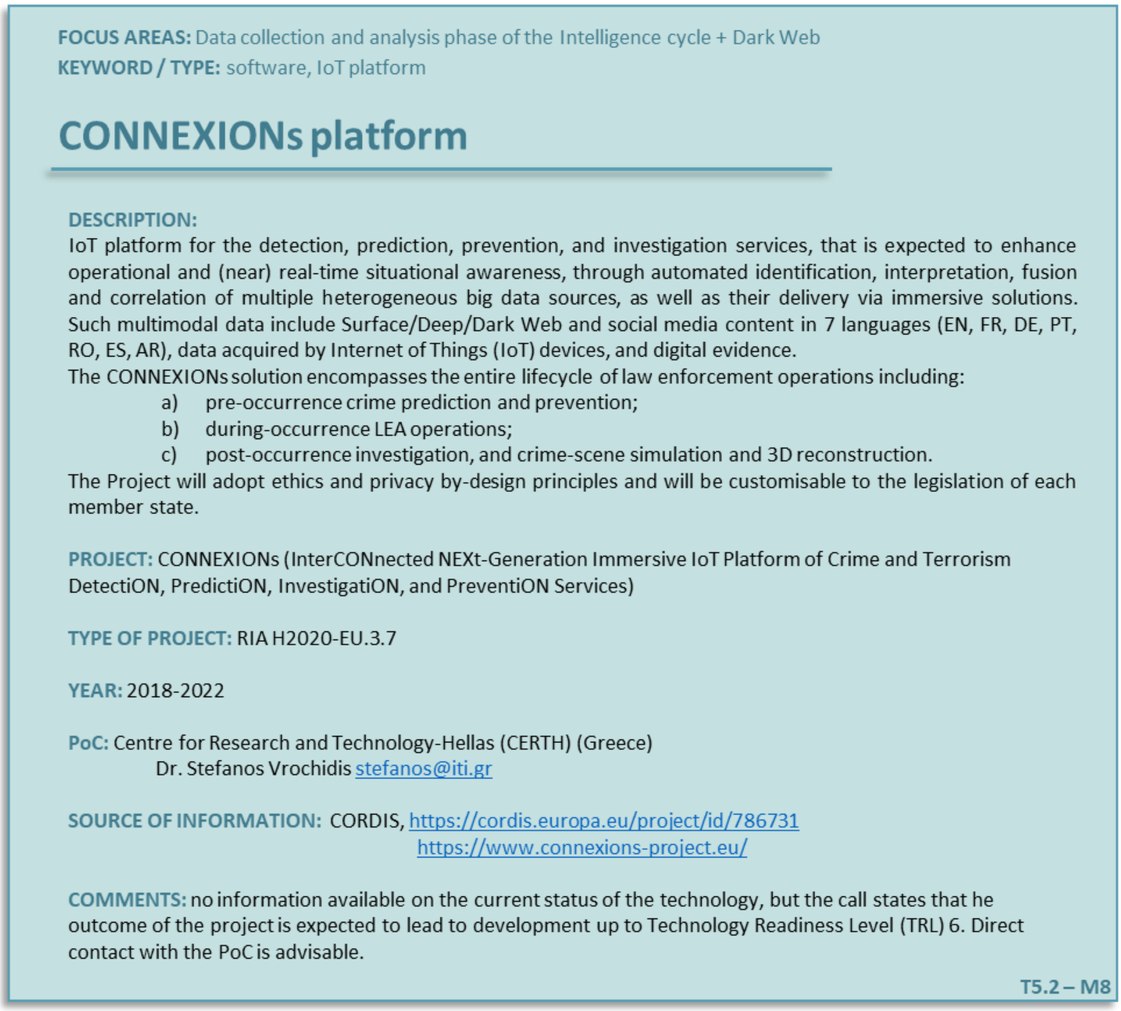
In the meanwhile, the 80% of the total EU Funding is claimed from only 9 Countries: Germany, France, Italy, Spain, Greece, Netherland, UK, Belgium and Austria.

4. Main findings

This section presents the main findings of the research described in the previous sections of this document. The common layout for the summarization of the information proposed in deliverable D5.1 is used.

CONNEXIONs Platform

CONNEXIONs (InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services) is a RIA that started in 2018 and ended in February 2022. It developed a Platform to help LEAs fight radicalization on surface, deep and dark web as well as in social media content in seven languages (EN, FR, DE, PT, RO, ES, AR):



FOCUS AREAS: Data collection and analysis phase of the Intelligence cycle + Dark Web
KEYWORD / TYPE: software, IoT platform

CONNEXIONs platform

DESCRIPTION:
IoT platform for the detection, prediction, prevention, and investigation services, that is expected to enhance operational and (near) real-time situational awareness, through automated identification, interpretation, fusion and correlation of multiple heterogeneous big data sources, as well as their delivery via immersive solutions. Such multimodal data include Surface/Deep/Dark Web and social media content in 7 languages (EN, FR, DE, PT, RO, ES, AR), data acquired by Internet of Things (IoT) devices, and digital evidence.
The CONNEXIONs solution encompasses the entire lifecycle of law enforcement operations including:

a) pre-occurrence crime prediction and prevention;
b) during-occurrence LEA operations;
c) post-occurrence investigation, and crime-scene simulation and 3D reconstruction.

The Project will adopt ethics and privacy by-design principles and will be customisable to the legislation of each member state.

PROJECT: CONNEXIONs (InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services)

TYPE OF PROJECT: RIA H2020-EU.3.7

YEAR: 2018-2022

PoC: Centre for Research and Technology-Hellas (CERTH) (Greece)
Dr. Stefanos Vrochidis stefanos@iti.gr

SOURCE OF INFORMATION: CORDIS, https://cordis.europa.eu/project/id/786731
https://www.connexions-project.eu/

COMMENTS: no information available on the current status of the technology, but the call states that he outcome of the project is expected to lead to development up to Technology Readiness Level (TRL) 6. Direct contact with the PoC is advisable.

T5.2 – M8

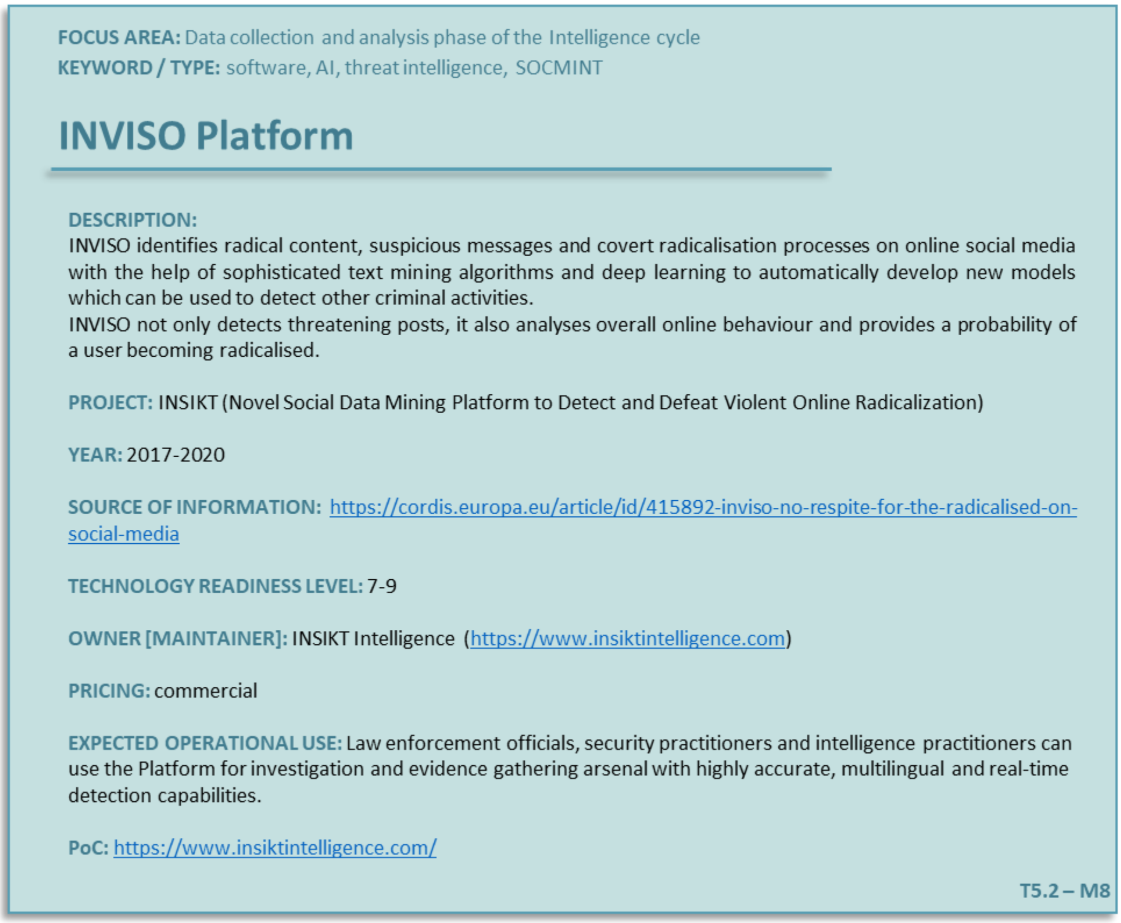
CONNEXIONs has several sister projects[15]: AIDA [31], ANITA [32], AP4AI [33], APPRAISE [34], CREST [35], INFINITY [36], LETSCROWD [37], MAGNETO [38], PREVISION [39], PROPHETS [40], PROTON [41], RED-Alert [42], REBORDER [43], ROXANNE [44], SHOTPROS [45], VICTORIA [46], all in the same cluster of projects.

[15] https://www.connexions-project.eu/sister-projects

NOTIONES should investigate if practitioners are interested in some of the technologies developed by these projects, keeping in mind that these were developed specifically for LEAs, and in this regard security and intelligence practitioners may have requirements different from those of LEAs.

INVISO Platform

INVISO is a SOCMINT (SOCial Media INTelligence) Platform that detects and foresees online radicalization. It is already a commercialized product, by company INSIKT Intelligence[16] based in Barcelona, Spain. The Platform was enhanced thanks to EU funding between years 2017 and 2020:



FOCUS AREA: Data collection and analysis phase of the Intelligence cycle
KEYWORD / TYPE: software, AI, threat intelligence, SOCMINT

INVISO Platform

DESCRIPTION:
INVISO identifies radical content, suspicious messages and covert radicalisation processes on online social media with the help of sophisticated text mining algorithms and deep learning to automatically develop new models which can be used to detect other criminal activities.
INVISO not only detects threatening posts, it also analyses overall online behaviour and provides a probability of a user becoming radicalised.

PROJECT: INSIKT (Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization)

YEAR: 2017-2020

SOURCE OF INFORMATION: https://cordis.europa.eu/article/id/415892-inviso-no-respite-for-the-radicalised-on-social-media

TECHNOLOGY READINESS LEVEL: 7-9

OWNER [MAINTAINER]: INSIKT Intelligence (https://www.insiktintelligence.com)

PRICING: commercial

EXPECTED OPERATIONAL USE: Law enforcement officials, security practitioners and intelligence practitioners can use the Platform for investigation and evidence gathering arsenal with highly accurate, multilingual and real-time detection capabilities.

PoC: https://www.insiktintelligence.com/

T5.2 – M8

Although no updated information was found about the INVISO technology, the INSIKT Intelligence company's website offers a rich portfolio of software products for OSINT and SOCMINT.

NOTIONES should contact INSIKT Intelligence and ask for a DEMO of their main products so that practitioners can understand what they are about, discuss if they may need it and elaborate on which modifications would be required to adapt a certain product to their operational and technical needs.

mh SERVICE GmbH Web-I-Qube

mh SERVICE GmbH[17] is a company headquartered in Kandel, in the South-West Germany. They were coordinators of the DAN project, a SME-1 H2020 project which developed a high-performance, kiosk-

[16] https://www.insiktintelligence.com/
[17] https://www.mh-service.de/en

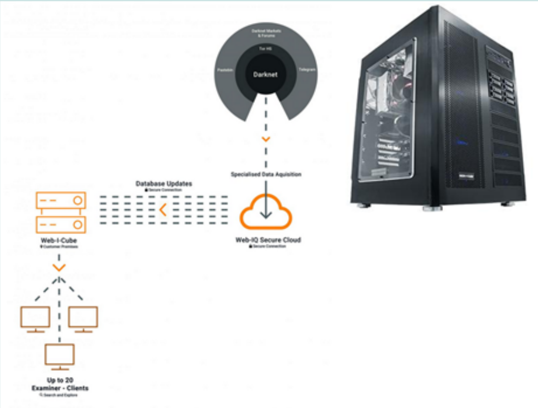
solution for forensic darknet analysis to gain cyber threat intelligence for companies and greatly enhance efficiency and capabilities of European investigation authorities.

Although no updated information was found about the DAN technology, the company's website offers a rich portfolio of products for investigations and digital forensics, both software and hardware, including the product Web-I-Qube [47] for the analysis of darknet content:

FOCUS AREA: monitoring and collecting data from the dark web
KEYWORD / TYPE: software, hardware, dark web Intelligence

Web-I-Qube

DESCRIPTION:
This solution is optimised for the analysis of social networks, the Darknet and its markets, enables targeted profiling and better analysis of general market trends. Automated risk scores help to set priorities for faster investigation results. This hardware-software combination even allows offline analysis of the Darknet by providing up-to-date data and login information of Darknet forums and markets, the user can regularly download a complete summary (or Data-Set) to the WebIQube server and analyse it offline. So there is no need to log in to the Darknet. The analysis tool supports full text search and advanced filtering like date range queries, geo location filters, category selections on documents, images, videos, posts, user profiles, websites etc.



YEAR: 2022

SOURCE OF INFORMATION: https://www.mh-service.de/en/products/web-i-qube

TECHNOLOGY READINESS LEVEL: 9 (Actual system proven in operational environment)

OWNER [MAINTAINER]: mh SERVICE Gmbh (Germany)

PRICING: commercial

EXPECTED OPERATIONAL USE: the platform allows to analyse online content offline, which can be required by law, or helpful when working in sensitive or specialist areas such as child pornography or terrorism

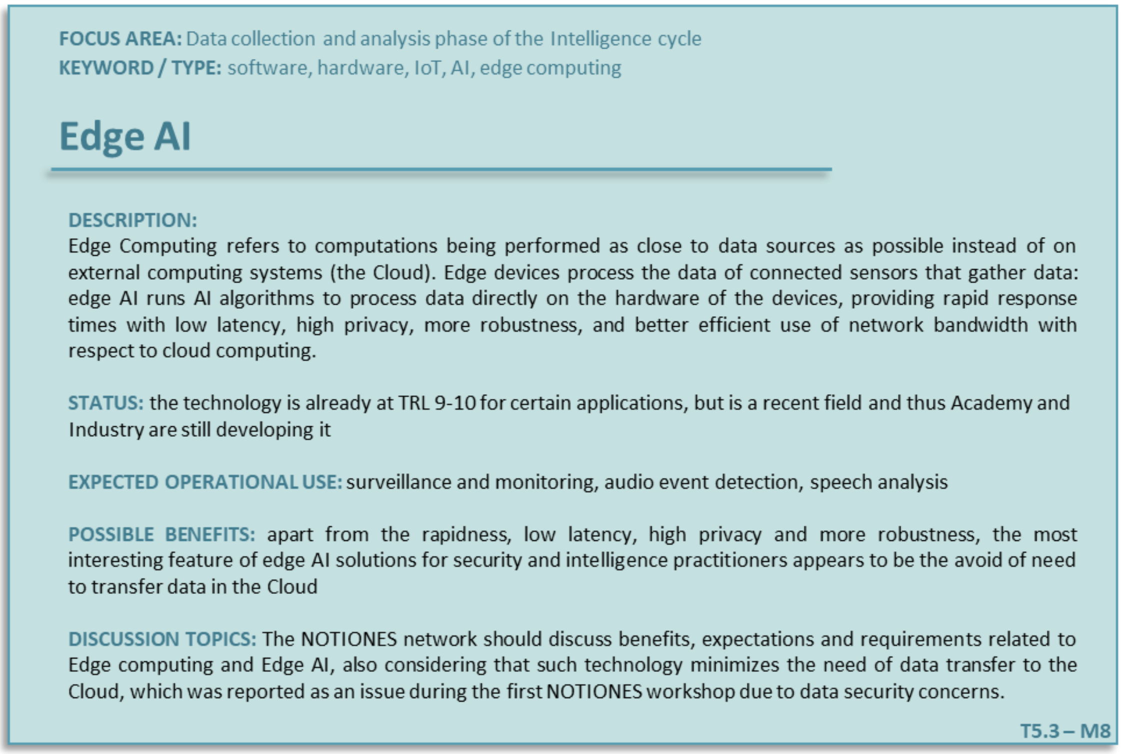
T5.2 – M8

NOTIONES should inform practitioners interested in dark web analysis and monitoring of the existence of this kind of technologies, although being it already a commercialized product the degree of possible adaptation of the product to the needs of the practitioners themselves is not clear.

Edge AI

Internet of Things and the rise of Big Data, data processing and machine learning applications are being moved to cheap and low size, weight, and power (SWaP) devices at the edge, often in the form of mobile phones, embedded systems, or microcontrollers. The field of Cyber-Physical Measurements and Signature Intelligence (MASINT) uses these devices to analyse and exploit data in ways not otherwise possible, which results in increased data quality, increased security, and decreased bandwidth. Applications range from Surveillance and Monitoring, to Audio Event Detection, to Speech analysis and many others.

During the first workshop of NOTIONES (task T7.1) and the first working groups (task T6.1) the topic of transferring data used by LEAs in external servers, often in foreign countries, was recognised as a key issue. Edge AI may help solve this problem by significantly decrease the need of such data transfer, allowing to collect and process data locally, in real time:



FOCUS AREA: Data collection and analysis phase of the Intelligence cycle
KEYWORD / TYPE: software, hardware, IoT, AI, edge computing

Edge AI

DESCRIPTION:
Edge Computing refers to computations being performed as close to data sources as possible instead of on external computing systems (the Cloud). Edge devices process the data of connected sensors that gather data: edge AI runs AI algorithms to process data directly on the hardware of the devices, providing rapid response times with low latency, high privacy, more robustness, and better efficient use of network bandwidth with respect to cloud computing.

STATUS: the technology is already at TRL 9-10 for certain applications, but is a recent field and thus Academy and Industry are still developing it

EXPECTED OPERATIONAL USE: surveillance and monitoring, audio event detection, speech analysis

POSSIBLE BENEFITS: apart from the rapidness, low latency, high privacy and more robustness, the most interesting feature of edge AI solutions for security and intelligence practitioners appears to be the avoid of need to transfer data in the Cloud

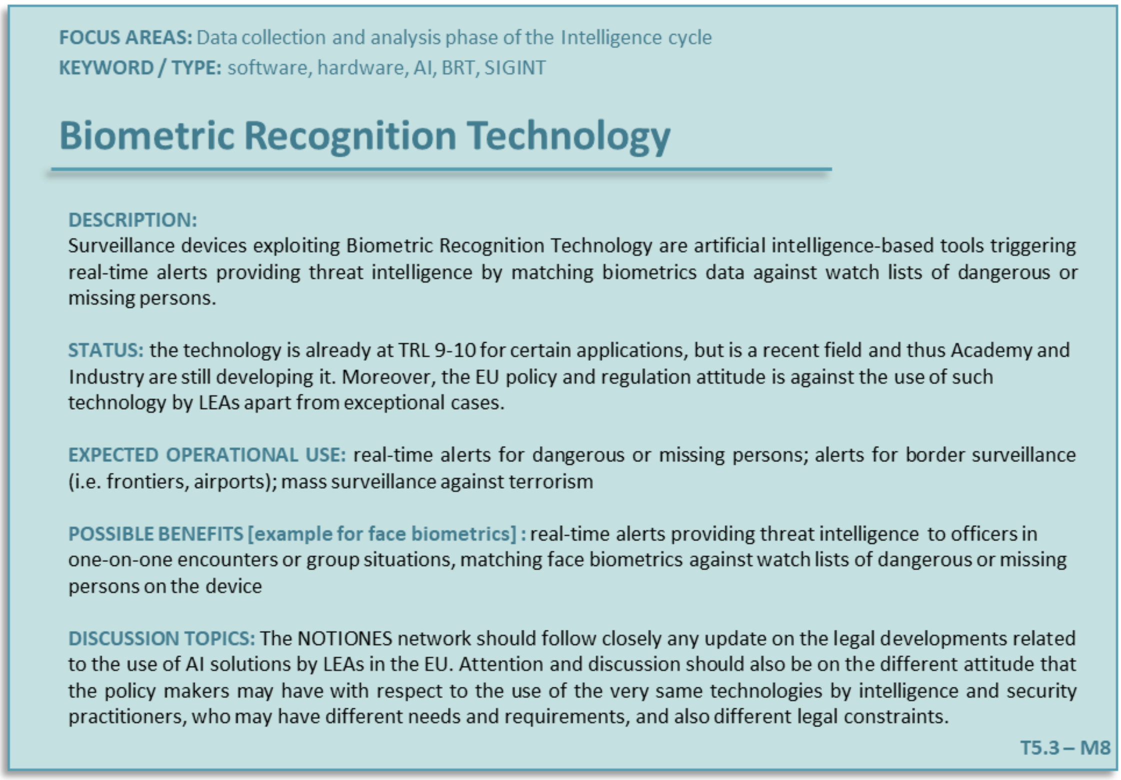
DISCUSSION TOPICS: The NOTIONES network should discuss benefits, expectations and requirements related to Edge computing and Edge AI, also considering that such technology minimizes the need of data transfer to the Cloud, which was reported as an issue during the first NOTIONES workshop due to data security concerns.

T5.3 – M8

Biometric Recognition Technology

Biometric recognition technologies are promising in the field of surveillance and in the field of security in general. Although such technologies are not mature yet, algorithms are becoming increasingly efficient and accurate. Likewise, ethical concerns are also increasing and the EU policy makers are reasoning on how to develop regulations balancing both civil rights protection and security-related legitimate use of such technologies.

Two results are presented, for the generic technology and for the voice-biometrics project SiiP:



FOCUS AREAS: Data collection and analysis phase of the Intelligence cycle

KEYWORD / TYPE: software, hardware, AI, BRT, SIGINT

Biometric Recognition Technology

DESCRIPTION:
Surveillance devices exploiting Biometric Recognition Technology are artificial intelligence-based tools triggering real-time alerts providing threat intelligence by matching biometrics data against watch lists of dangerous or missing persons.

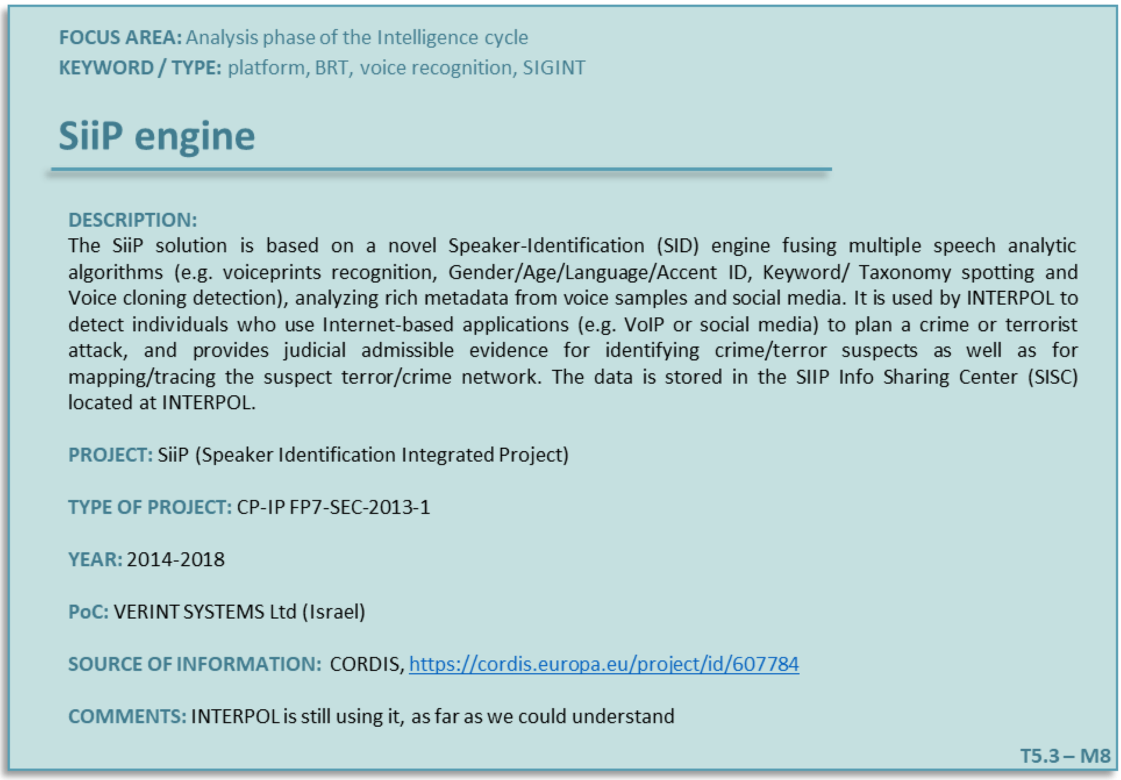
STATUS: the technology is already at TRL 9-10 for certain applications, but is a recent field and thus Academy and Industry are still developing it. Moreover, the EU policy and regulation attitude is against the use of such technology by LEAs apart from exceptional cases.

EXPECTED OPERATIONAL USE: real-time alerts for dangerous or missing persons; alerts for border surveillance (i.e. frontiers, airports); mass surveillance against terrorism

POSSIBLE BENEFITS [example for face biometrics] : real-time alerts providing threat intelligence to officers in one-on-one encounters or group situations, matching face biometrics against watch lists of dangerous or missing persons on the device

DISCUSSION TOPICS: The NOTIONES network should follow closely any update on the legal developments related to the use of AI solutions by LEAs in the EU. Attention and discussion should also be on the different attitude that the policy makers may have with respect to the use of the very same technologies by intelligence and security practitioners, who may have different needs and requirements, and also different legal constraints.

T5.3 – M8



FOCUS AREA: Analysis phase of the Intelligence cycle

KEYWORD / TYPE: platform, BRT, voice recognition, SIGINT

SiiP engine

DESCRIPTION:
The SiiP solution is based on a novel Speaker-Identification (SID) engine fusing multiple speech analytic algorithms (e.g. voiceprints recognition, Gender/Age/Language/Accent ID, Keyword/ Taxonomy spotting and Voice cloning detection), analyzing rich metadata from voice samples and social media. It is used by INTERPOL to detect individuals who use Internet-based applications (e.g. VoIP or social media) to plan a crime or terrorist attack, and provides judicial admissible evidence for identifying crime/terror suspects as well as for mapping/tracing the suspect terror/crime network. The data is stored in the SIIP Info Sharing Center (SISC) located at INTERPOL.

PROJECT: SiiP (Speaker Identification Integrated Project)

TYPE OF PROJECT: CP-IP FP7-SEC-2013-1

YEAR: 2014-2018

PoC: VERINT SYSTEMS Ltd (Israel)

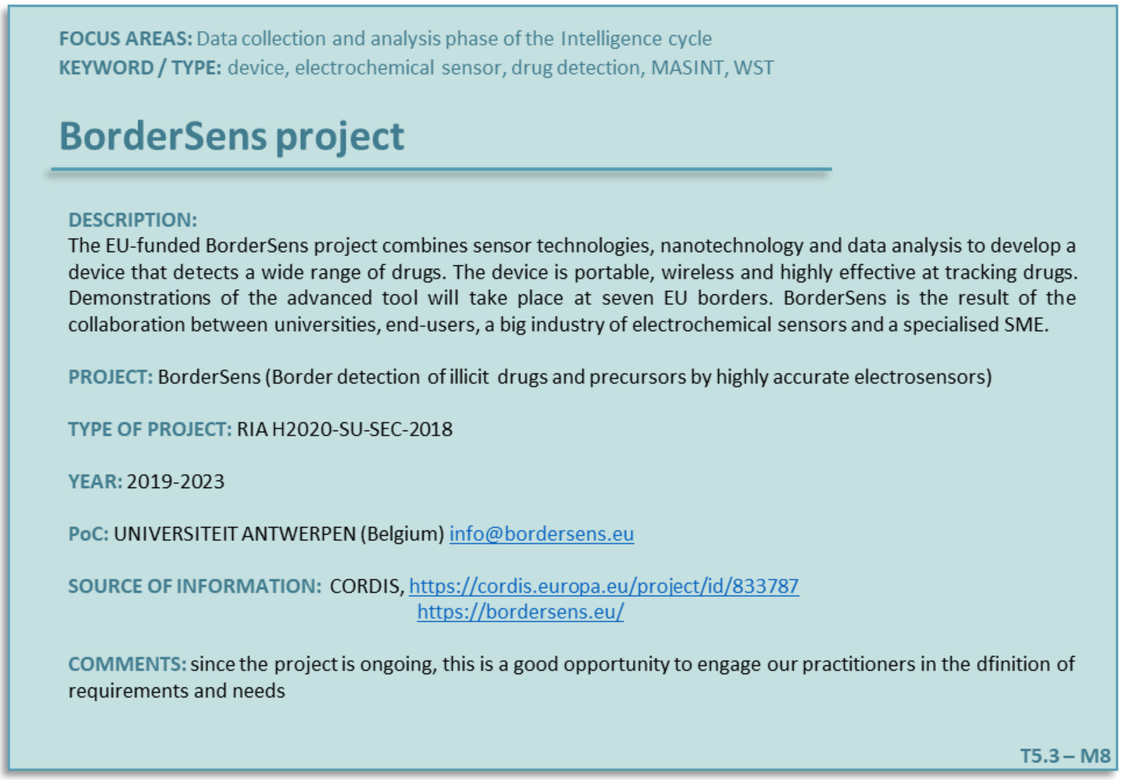
SOURCE OF INFORMATION: CORDIS, https://cordis.europa.eu/project/id/607784

COMMENTS: INTERPOL is still using it, as far as we could understand

T5.3 – M8

Wearable Sensor Technology

Wearable sensor technologies are promising in the fields of health and safety monitoring, as well as CBRN detection. Authoritative reports already exist about the requirements of LEAs for the use of such technology. NOTIONES is called upon to carry out similar evaluations and analyses to security and intelligence practitioners, using existing reports as a yardstick to assess differences with respect to the LEAs' perspective. A good opportunity is to interact and collaborate, for example, with the BorderSens project.



FOCUS AREAS: Data collection and analysis phase of the Intelligence cycle
KEYWORD / TYPE: device, electrochemical sensor, drug detection, MASINT, WST

BorderSens project

DESCRIPTION:
The EU-funded BorderSens project combines sensor technologies, nanotechnology and data analysis to develop a device that detects a wide range of drugs. The device is portable, wireless and highly effective at tracking drugs. Demonstrations of the advanced tool will take place at seven EU borders. BorderSens is the result of the collaboration between universities, end-users, a big industry of electrochemical sensors and a specialised SME.

PROJECT: BorderSens (Border detection of illicit drugs and precursors by highly accurate electrosensors)

TYPE OF PROJECT: RIA H2020-SU-SEC-2018

YEAR: 2019-2023

PoC: UNIVERSITEIT ANTWERPEN (Belgium) info@bordersens.eu

SOURCE OF INFORMATION: CORDIS, https://cordis.europa.eu/project/id/833787
https://bordersens.eu/

COMMENTS: since the project is ongoing, this is a good opportunity to engage our practitioners in the dfinition of requirements and needs

T5.3 – M8

Internet of Things

IoT hacking, interception and forensics is a challenging field as the IoT security landscape evolves. Practitioners of the NOTIONES network should be informed about recently developed solutions in order to be able to perform specific training of the personnel.

Also, IoT devices may bring substantial benefits to practitioners in the field, but security issues must be solved before large-scale use. The approach here appears similar to the one proposed for WSTs.

Dark Net threat categorisation

Software for the monitoring of illicit activities on the Dark Web has been produced and used by LEAS in the past, but new algorithms are being developed every day.

The NOTIONES practitioners should discuss if they are aware of such tools and if they are willing to use them, being aware that specialized personnel must be trained and that specific algorithms are needed for each operational task.

5. Conclusions and next steps

In conclusion, the results of the first run of tasks T5.2 and T5.3 were documented in this report. Findings are summarised in section 4, highlighting the technologies and EU projects that are promising for the purposes of NOTIONES.

The main results were also added in the NOTIONES CTI Catalogue on the online project SharePoint and the information was also forwarded to WP6, in order to feed the Working Groups.

With regard to the next steps, two main actions are foreseen in the next runs of tasks T5.2 and T5.3 in months M12-M14:

- After the feedback from the working groups, T5.2 will further investigate the most interesting projects by contacting the coordinators, exchanging information and promoting interaction. This will be made mainly through the task contributors TECNA, Z&P, LAU, BDI, SAHER, SYNYO and KhNUIA, who will act as Points of Contact.
- The research of T5.2 will be repeated on CORDIS after the Horizon Europe project proposals' evaluation.
- After the feedback from the working groups, T5.3 will further investigate the most interesting technologies by contacting the technology providers, exchanging information and promoting interaction. This will be made mainly through the task contributors TECNA, DRI, EXPSYS and SAHER, who will act as Points of Contact.
- New research topics will be targeted in the next run of the tasks, corresponding to the new focus areas tackled by upcoming working groups.

Updates will be included in the next release of the deliverable D5.3 "*Monitoring of EU Research and Horizon Scanning -v2*", due in M14.

References

[1] D. Rotolo, D. Hicks and B. R. Martin, “What Is an Emerging Technology?,” *Research Policy,* vol. 44, no. 10, pp. 1827-1843, 9 August 2015.

[2] Commission Decision C(2017)7124, “Technology readiness levels (TRL),” HORIZON 2020 – WORK PROGRAMME 2018-2020 General Annexes Extract from Part 19, 2017.

[3] TheLens. [Online]. Available: https://www.lens.org/.

[4] Publications Office of the European Union, “COmmunity Research and Development Information Service,” [Online]. Available: https://cordis.europa.eu/en.

[5] D. Elliott, “Efficient Edge Analytics: Addressing Cyber-Physical MASINT with Machine Learning on Audio at the Edge,” Thesis (Ph.D.) - Florida Institute of Technology, 2020.

[6] viso.ai, “Edge AI – Driving Next-Gen AI Application,” 2022. [Online]. Available: https://viso.ai/edge-ai/edge-ai-applications-and-trends/ .

[7] Forbes, “The Edge: What Does It Mean For Artificial Intelligence?,” 9 January 2021. [Online]. Available: https://www.forbes.com/sites/tomtaulli/2021/01/09/the-edge-what-does-it-mean-for-ai-artificial-ingelligence/?sh=245cb92063f3 .

[8] STMicroelectronics, “Some Use cases for AI on the Edge,” 2022. [Online]. Available: https://www.st.com/content/st_com/en/about/innovation---technology/image-analytics.html.

[9] F. Jansen, J. Sánchez-Monedero and L. Dencik, “Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP,” *Big Data & Society,* vol. 8, no. 2, 2021.

[10] SiiP, “SiiP,” 2014-2018. [Online]. Available: https://cordis.europa.eu/project/id/607784/it.

[11] INTERPOL, “SiiP,” 2022. [Online]. Available: https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP.

[12] M. P. J. R. S. N. F. M. A. B. R. V. E. Hazhir Teymourian, K. D. Wael and J. Wang, “Wearable Electrochemical Sensors for the Monitoring and Screening of Drugs,” *ACS sensors,* vol. 5, no. 9, pp. 2679-2700, 2020.

[13] BorderSens, “BorderSens,” 2019-2023. [Online]. Available: https://cordis.europa.eu/project/id/833787.

[14] BorderSens, “publications,” [Online]. Available: https://bordersens.eu/project-results/.

[15] L. J. Hubble and J. Wang, “Wearable Electrochemical Sensors for Rapid and on-Site Chemical Threat Assessment,” *ECS Meeting Abstracts,* Vols. MA2020-01, no. 27, pp. 2003-2003, 2020.

[16] S. E. Goodison, J. D. Barnum, M. J. D. Vermeer, D. Woods, S. I. Sitar, S. R. Shelton and B. A. Jackson, “Wearable Sensor Technology and Potential Uses Within Law Enforcement: Identifying High-

Priority Needs to Improve Officer Safety, Health, and Wellness Using Wearable Sensor Technology," RAND Corporation, 2020.

[17] A. MacDermott, T. Baker, P. Buck, F. Iqbal and Q. Shi, "The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics," *International Journal of Digital Crime and Forensics,* vol. 12, no. 1, pp. 1-13, 2020.

[18] National Institute of Standards and Technology, "trustworthy netoworks of things," 2022. [Online]. Available: https://www.nist.gov/programs-projects/trustworthy-networks-things.

[19] Internet Engineering Task Force, "IoT," [Online]. Available: https://www.ietf.org/topics/iot/.

[20] H. Atlam, A. Alenezi, M. Alassafi, A. Alshdadi and G. Wills, Security, Cybercrime and Digital Forensics for IoT, 2020.

[21] S. Mrdovic, "IoT Forensics," in *Security of Ubiquitous Computing Systems*, Springer, 2021, pp. 215-229.

[22] J. Toldinas, A. Venčkauskas, Š. Grigaliūnas, R. Damaševičius and V. Jusas, "Suitability of the digital forensic tools for investigation of cyber crime in the internet of things and services," *The 3rd International Virtual Research Conference In Technical Disciplines,* p. 86–97, 2015.

[23] D. Shah, T. G. Harrison, C. B. Freas, D. Maimon and R. W. and Harrison, "Illicit Activity Detection in Large-Scale Dark and Opaque Web Social Networks," *EBCS Articles,* vol. 20, 2021.

[24] H. Zhang and F. Zou, "A Survey of the Dark Web and Dark Market Research," *IEEE 6th International Conference on Computer and Communications (ICCC),* pp. 1694-1705, 2020.

[25] S. Ghosh, P. Porras, V. Yegneswaran, K. Nitz and A. Das, "ATOL: A Framework for Automated Analysis and Categorization of the Darkweb Ecosystem," *AAAI Workshops,* 2017.

[26] R. Rawat, V. Mahor, S. Chirgaiya, R. Shaw and A. Ghosh, "Analysis of Darknet Traffic for Criminal Activities Detection Using TF-IDF and Light Gradient Boosted Machine Learning Algorithm," in *Innovations in Electrical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 756*, Singapore, Springer, 2021, pp. 671-681.

[27] V. Mahor, R. Rawat, A. Kumar, M. Chouhan and R. N. S. A. Ghosh, "Cyber Warfare Threat Categorization on CPS by Dark Web Terrorist," *IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON),* pp. 1-6, 2021.

[28] S. Nazah, S. Huda, J. Abawajy and M. M. Hassan, "Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach," *IEEE Access,* vol. 8, pp. 171796-171819, 2020.

[29] C. Bradley, "On the Resilience of the Dark Net Market Ecosystem to Law Enforcement Intervention," University College London, 2019.

[30] Europol, "news," 2022. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom.

[31] H2020, "AIDA," [Online]. Available: https://www.project-aida.eu/.

[32] H2020, "ANITA," [Online]. Available: https://www.anita-project.eu/ .

[33] H2020, “AP4AI,” [Online]. Available: https://www.ap4ai.eu/.

[34] H2020, “APPRAISE,” [Online]. Available: https://appraise-h2020.eu/ .

[35] H2020, “CREST,” [Online]. Available: https://project-crest.eu/ .

[36] H2020, “INFINITY,” [Online]. Available: https://h2020-infinity.eu/ .

[37] H2020, “LETSCROWD,” [Online]. Available: https://letscrowd.eu/.

[38] H2020, “MAGNETO,” [Online]. Available: http://www.magneto-h2020.eu/.

[39] H2020, “PREVISION,” [Online]. Available: http://www.prevision-h2020.eu/.

[40] H2020, “PROPHETS,” [Online]. Available: https://www.prophets-h2020.eu/.

[41] H2020, “PROTON,” [Online]. Available: https://www.projectproton.eu.

[42] H2020, “RED-Alert,” [Online]. Available: http://redalertproject.eu/.

[43] H2020, “REBORDER,” [Online]. Available: https://roborder.eu/.

[44] H2020, “ROXANNE,” [Online]. Available: https://www.roxanne-euproject.org/.

[45] H2020, “SHOTPROS,” [Online]. Available: https://shotpros.eu/.

[46] H2020, “VICTORIA,” [Online]. Available: https://www.victoria-project.eu/.

[47] mh SERVICE Gmbh, “Web-I-Qube,” 2022. [Online]. Available: https://www.mh-service.de/en/products/web-i-qube.

[48] European Commission, “White Paper on Artificial Intelligence - A European approach to excellence and trust COM(2020) 65 final,” Brussels, 2020.

[49] COM(2021) 206 final 2021/0106 (COD), “Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Articicial Intelligence Act) and amending certain Union legislative acts,” European Parliament, Brussels, 2021.

[50] Squire Patton Boggs, “The proposed new EU regulatory regime for Artificial Intelligence,” September 2021.

[51] Regulation (EU) 2016/679, “General Data Protection Regulation,” EU, 2016.

[52] Columbia Journal of Transnational Law, “Europe’s Next Steps in Regulating Facial Recognition Technology,” November 2021. [Online]. Available: https://www.jtl.columbia.edu/bulletin-blog/europes-next-steps-in-regulating-facial-recognition-technology.

[53] MEP, “Letter to the European Commission,” European Parliament, Brussels, 8 March 2021.

[54] European Data Protection Board, “Press Release statement,” May 2021. [Online]. Available: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

[55] European Parliamentary Research Service, “Regulating facial recognition in the EU,” 2021.

[56] Official Journal of the European Communities, “Charter of the Fundamental Rights of the European Union (2000/C 364/01),” 2000.

[57] European Parliament, “Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [...],” 2016.

[58] European Parliament, “Press Releases,” 6 October 2021. [Online]. Available: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.

Annex I: Artificial Intelligence Act

In February 2020 the European Commission published a White Paper on Artificial Intelligence [48], highlighting the fundamental rights implications of using remote biometric identification AI systems, and especially Face Recognition Technologies (FRTs).

In April 2021 the EU Commission published a proposal for Regulation laying down Harmonised Rules on Artificial Intelligence (**Artificial Intelligence Act** – AIA) [49], attempting to give a comprehensive legal framework for the use of AI. This proposed regulation proposes a risk-based categorisation of AI systems with four levels of risk and related regulatory obligations and restrictions.

Most AI uses are left free from regulation, but a very limited number of particularly harmful high-risk AI practices that contravene the EU values are **prohibited**: social scoring by governments, exploiting vulnerabilities of children or disabled persons, using subliminal techniques that can cause physical or psychological harm and **live remote biometric identification systems used by LEAs in public places**.

Remote biometrics identification systems, including Facial Recognition Technologies (FRTs), are systems that operate at a distance without knowing whether the relevant person will be present in the area, capture biometric data (including through facial image recognition), compare it with an existing sample or database without significant delay and are used for identifying an individual (recital 8 and Article 3(33) of [49]).

The AIA allows the use of such technologies for Law Enforcement purposes in publicly accessible spaces only in the following **exceptional cases**:

- 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 [50].

It should be recalled here that the 2016 General Data Protection Regulation (GDPR, [51]) considers biometric data as personal data because they are "*factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*", and as such the biometric data of EU citizens and long-term residents cannot be shared with third parties without their explicit consent. The GDPR does contain some exceptions to this requirement: for example, if the information is necessary for employment, social security, and social protection law, or if it is crucial to the public interest in public health.

A cross-party group of 40 members of the European Parliament attacked the AIA's overall approach as too weak in countering the broad risks posed by facial recognition technology. Also, the *Reclaim Your Face* advocacy coalition, formed by 60 European human rights and social justice groups, raised objections to the draft proposal, considering it too narrowly focused on law enforcement use, thereby "failing to prohibit equally invasive and dangerous uses by other government authorities as well as by private companies" [52]. In March 2021, a group of more than a hundred members of the European Parliament called on the EC to enshrine an explicit ban on biometric mass surveillance in public spaces in EU law [53].

In June 2021, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski urged a general ban on "any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context" and raised a growing concern at the intersection of surveillance law and human rights law, calling for a "precautionary approach" to the future of FRT [54].

In September 2021 the European Parliamentary Research Service (EPRS) published the "Regulating facial recognition in the EU" report [55], rising concerns about the risk of error of FTR systems. A false negative occurs when the system fails to find a face that is present on a picture, while a false negative occurs when it identifies a non-face structure as a real face. Error rates can be significant due to pictures taken in different conditions of light, shadow, background etc. Moreover, insufficient training data is another cause of error. In the view of the EPRS, "*these risks may have very far-reaching consequences for fundamental rights*". In addition to possible errors, although there are real benefits to using FRT in terms of public safety, security and efficiency for identity verification the use of FRT technologies by LEAs, this may lead to indiscriminate mass surveillance, breaching the fundamental rights to data protection, privacy and non-discrimination which enshrine a set of basic guarantees at the primary level in the Charter of Fundamental Rights (CFR) [56].

It should also be recalled here that the Law Enforcement Directive (LED) [57] is the applicable directive when public authorities and LEAs process personal data for the prevention, investigation, detection and prosecution of criminal offences.

In this legal framework, the processing of facial images must comply with the following:

- It must be lawful, fair and transparent (Articles 5(1)(a) GDPR, Article 4(1)(a) LED, Recital 26 LED);
- It must follow a specific, explicit and legitimate purpose (Article 5(1)(b) GDPR, Article 4(1)(b) LED);
- Comply with the requirements of data minimisation (Article 5(1)(c) GDPR, Article 4(1)(c) LED), data accuracy (Article 5(1)(d) GDPR, Article 4(1)(d) LED), storage limitation (Article 5(1)(e) GDPR, Article 4(1)(e) LED), data security (Article 5(1)(f) GDPR, Article 4(1)(f) LED) and accountability (Article 5(2) GDPR, Article 4(4) LED).

The EPRS also highlighted that "*FRTs need to take into account of requirements under EU law protecting the rights of the child and of elderly people, the freedom of expression and freedom of assembly and of association, the right to good administration, as well as the right to an effective remedy*". Other concerns relate to "*product safety, product liability and consumer protection*" and compliance with the growing body of EU law governing border control.[18]

In October 2021, the European Parliament passed a nonbinding resolution that bans the police use of facial recognition in public places and the creation of private facial recognition databases, signalling the EP's view on the matter [58].

The draft AI regulation will continue to undergo debate and review by the European Parliament and the Member States through the European Council. In the meantime, the delicate balance between privacy, innovation, and surveillance will undoubtedly continue to be debated in the European Parliament and in other jurisdictions [52]. Next to the current legislative debates, the EC will, in 2022, come forward with additional legislative measures regarding AI, focused on adapting the liability framework to be applied to emerging technologies. This will likely include a revision of the Product Liability Directive, and a legislative proposal related to the liability of AI systems [50].

[18] For example, the integration of automatic FRT in the EU Schengen Information System (SIS) has been proposed

Annex II: List of researched EU projects

Project	EU-HYBNET
Full Title	Empowering a Pan-European Network to Counter Hybrid Threats
GRANT AGREEMENT ID:	883054
Source of information	SU-GM01-2018-2019-2020 - Pan-European networks of practitioners and other actors in the field of security
Call for Proposal	H2020-SU-SEC-2019
EU contribution	€ 3 496 837,50
Coordinator	LAUREA-AMMATTIKORKEAKOULU OY / Finland
Website:	https://www.laurea.fi/en/projects/e/empowering-a-pan-european-network-to-counter-hybrid-threats/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/991816077/883054
Funding Scheme	Coordination and Support Action (CSA)
Start Date	1/05/2021
End Date	30/04/2025
Description of any problem encountered	NOTIONES partner LAUREA is the coordinator

Project	POP AI
Full Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights
GRANT AGREEMENT ID:	101022001
Source of information	SU-AI03-2020 - Human factors, and ethical, societal, legal and organisational aspects of using Artificial Intelligence in support of Law Enforcement
Call for Proposal	H2020-SU-AI-2020
EU contribution	245 000
Coordinator	"NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS/Greece
Website:	https://www.demokritos.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999978239/101022001
Funding Scheme	Coordination and Support Action (CSA)
Start Date	01/10/2021
End Date	30/09/2023
Description of any problem encountered	NOTIONES partner Z&P is in the consortium

Project	ALIGNER
Full Title	Developing a research roadmap regarding Artificial Intelligence Roadmap for Policing and Law Enforcement
GRANT AGREEMENT ID:	101020574
Source of information	SU-AI01-2020 - Developing a research roadmap regarding Artificial Intelligence in support of Law Enforcement
Call for Proposal	H2020-SU-AI-2020
EU contribution	€ 1 499 960
Coordinator	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V /D
Website:	https://www.fraunhofer.de/ Hansastrasse 27C 80686 Munchen Germany

Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999984059/101020574
Funding Scheme	Coordination and Support Action (CSA)
Start Date	01/10/2021
End Date	30/09/2024
Description of any problem encountered	No Coordinator name available, but just a contact form on CORDIS.

Project	LETS-CROWD
Full Title	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings
GRANT AGREEMENT ID:	740466
Source of information	SEC-07-FCT-2016-2017 - Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts
Call for Proposal	H2020-SEC-2016-2017-1
EU contribution	€ 417 612,50
Coordinator	ETRA INVESTIGACION Y DESARROLLO SA Calle Tres Forques 147 46014 Valencia Spain
Website:	https://www.grupoetra.com/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999926441/740466
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/05/2017
End Date	31/10/2019
Description of any problem encountered	

Project	STARLIGHT
Full Title	Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats
GRANT AGREEMENT ID:	101021797
Source of information	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
Call for Proposal	H2020-SU-AI-2020
EU contribution	€ 18 835 263,75
Coordinator	COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES, Rue Leblanc 25 75015 Paris 15 France
Website:	https://www.cea.fr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999992401/101021797
Funding Scheme	Innovation Action (IA)
Start Date	01/10/2021
End Date	30/09/2025
Description of any problem encountered	

Project	PREVISION
Full Title	Prediction and Visual Intelligence for Security Information
GRANT AGREEMENT ID:	833115
Source of information	SU-FCT03-2018-2019-2020 - Information and data stream management to fight against (cyber)crime and terrorism
Call for Proposal	H2020-SU-SEC-2018
EU contribution	€ 9 040 230,00
Coordinator	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS Patission Str. 42 10682 Athina Greece
Website:	https://www.iccs.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999654356/833115
Funding Scheme	IA - Innovation action
Start Date	01/09/2019
End Date	31/12/2021
Description of any problem encountered	

Project	ECHO
Full Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
GRANT AGREEMENT ID:	830943
Source of information	SU-ICT-03-2018 - Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap
Call for Proposal	H2020-SU-ICT-2018-2
EU contribution	15 987 285
Coordinator	ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL Avenue De La Renaissance 30 1000 Bruxelles Belgium
Website:	https://www.sic.rma.ac.be/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999831575/830943
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/02/2019
End Date	31/01/2023
Description of any problem encountered	NOTIONES partner Z&P is in the consortium

Project	SAPPAN
Full Title	Sharing and Automation for Privacy Preserving Attack Neutralization

GRANT AGREEMENT ID:	833418
Source of information	SU-ICT-01-2018 - Dynamic countering of cyber-attacks
Call for Proposal	H2020-SU-ICT-2018
EU contribution	€ 4 175 070
Coordinator	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV Hansastrasse 27C 80686 Munchen Germany
Website:	https://www.fraunhofer.de/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999984059/833418
Funding Scheme	Innovation Action (IA)
Start Date	01/05/2019
End Date	30/04/2022
Description of any problem encountered	

Project	REACT
Full Title	REactively Defending against Advanced Cybersecurity Threats
GRANT AGREEMENT ID:	786669
Source of information	DS-07-2017 - Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
Call for Proposal	H2020-DS-SC7-2017
EU contribution	€ 2 726 461,25
Coordinator	IDRYMA TECHNOLOGIAS KAI EREVNAS N Plastira Str 100 70013 Irakleio Greece
Website:	https://www.iceht.forth.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999995893/786669
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/06/2018
End Date	30/05/2021
Description of any problem encountered	

Project	REASSURE
Full Title	Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience
GRANT AGREEMENT ID:	731591
Source of information	DS-01-2016 - Assurance and Certification for Trustworthy and Secure ICT systems, services and components
Call for Proposal	H2020-DS-LEIT-2016
EU contribution	€ 831 624,61
Coordinator	UNIVERSITE CATHOLIQUE DE LOUVAIN

	Place De L Universite 1 1348 Louvain La Neuve Belgium
Website:	http://www.uclouvain.be/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999980664/731591
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/01/2017
End Date	31/03/2020
Description of any problem encountered	

Project	HoloZcan
Full Title	Deep Learning Powered Holographic Microscopy for Biothreat Detection on Field
GRANT AGREEMENT ID:	101021723
Source of Information	SU-DRS04-2019-2020 - Chemical, biological, radiological and nuclear (CBRN) cluster
Call for Proposal	H2020-SU-SEC-2020
EU contribution	€ 742 037,50
Coordinator	IDEAS SCIENCE KFT Oroszvar Utca 5. 1. Em 1173 Budapest Hungary
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/902471220/101021723
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/01/2017
End Date	31/03/2020
Description of any problem encountered	

Project	ENTRAP
Full Title	Enhanced Neutralisation of explosive Threats Reaching Across the Plot
Source of information	SEC-11-FCT-2016 - Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot
GRANT AGREEMENT ID:	740560
Call for Proposal	H2020-SEC-2016-2017-1
EU contribution	€ 1 655 868,75 against a total costs budget 4 978 248,75
Coordinator	TOTALFORSVARETS FORSKNINGSINSTITUT Gullfossgatan 6 164 90 Stockholm Sweden
Website:	https://www.foi.se/

Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999627875/740560
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/05/2017
End Date	31/10/2020
Description of any problem encountered	

Project	STAMINA
Full Title	Demonstration of intelligent decision support for pandemic crisis prediction and management within and across European borders
GRANT AGREEMENT ID:	883441
Source of information	Demonstration of intelligent decision support for pandemic crisis prediction and management within and across European borders | STAMINA Project | Fact Sheet | H2020 | CORDIS | European Commission (europa.eu)
EU contribution	€ 9. 494. 326,25 against a Total Cost of : € 11 020 801,25
Coordinator	EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS 73-75 Mesogion Avenue, 11526 Athens, Greece
Website:	https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d6750aac&appId=PPGMS
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/916943523/883441
Funding Scheme	Innovation Action (IA)
Start Date	1 September 2020
End Date	31 August 2021
Description of any problem encountered	

Project	CRiTERIA
Full Title	Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks
GRANT AGREEMENT ID:	101021866
Source of information	https://cordis.europa.eu/project/id/101021866
EU contribution	€ 4 890 177,50
Coordinator	GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET, Welfengarten 1, 30167 Hannover D
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999981828/101021866
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 September 2021
End Date	31 August 2024
Description of any problem encountered	

Project	Co-Inform
Full Title	Co-Creating Misinformation-Resilient Societies
GRANT AGREEMENT ID:	770302

Source of information	https://cordis.europa.eu/project/id/770302
EU contribution	€ 4 110 758,75
Coordinator	STOCKHOLMS UNIVERSITET Universitetsvagen 10 10691 Stockholm
Website:	http://www.su.se/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999885022/770302
Funding Scheme	Research and Innovation Action (RIA)
Start Date	01/04/2018
End Date	31/07/2021
Description of any problem encountered	

Project	TRANS-URBAN-EU-CHINA
Full Title	Transition towards urban sustainability through socially integrative cities in the EU and in China
GRANT AGREEMENT ID:	770141
Source of information	https://cordis.europa.eu/project/id/770141
EU contribution	€ 2 499 993,75
Coordinator	TECHNISCHE UNIVERSITAET DRESDEN Helmholtzstrasse 10 01069 Dresden
Website:	http://www.tu-dresden.de/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999897729/770141
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 January 2018
End Date	30 June 2021
Description of any problem encountered	

Project	LINSEC
Full Title	The Logic of Informal Security Cooperation: Counterterrorism Intelligence-sharing in Europe
GRANT AGREEMENT ID:	833120
Source of information	https://cordis.europa.eu/project/id/833120
EU contribution	€ 219 312
Coordinator	SYDDANSK UNIVERSITET, Campusvej 55 5230 Odense M, Danmark
Website:	http://www.sdu.dk/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999904616/833120
Funding Scheme	MSCA-IF-EF-ST - Standard EF
Start Date	1 September 2020
End Date	31 August 2022
Description of any problem encountered	

Project	APPRAISE

Full Title	fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts
GRANT AGREEMENT ID:	101021981
Source of information	https://cordis.europa.eu/project/id/101021981
EU contribution	€ 7 999 101,25 against a total cost of: € 9 427 982,50
Coordinator	CS GROUP-FRANCE, Avenue Galilee 22 92350 Le Plessis Robinson, F
Website:	http://www.c-s.fr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999938275/101021981
Funding Scheme	Innovation Action (IA)
Start Date	1 September 2021
End Date	31 August 2023
Description of any problem encountered	

Project	CyberSANE
Full Title	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
GRANT AGREEMENT ID:	833683
Source of information	https://cordis.europa.eu/project/id/833683/reporting
EU contribution	€ 4 985 550 against total costs of: € 6 146 737,50
Coordinator	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA, R Amadeu Sousa Cardoso 20 1 Dto 1300 066 Lisboa P
Website:	http://www.pdmfc.com/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999742335/833683
Funding Scheme	Innovation Action (IA)
Start Date	1 September 2019
End Date	31 August 2022
Description of any problem encountered	

Project	CONNEXIONs
Full Title	InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services
GRANT AGREEMENT ID:	786731
Source of information	https://cordis.europa.eu/project/id/786731
EU contribution	€ 4 999 390
Coordinator	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS, Charilaou Thermi Road 6 Km, 57001 Thermi Thessaloniki, Greece
Website:	http://www.certh.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/998802502/786731
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 September 2018
End Date	28 Feb 2022

Description of any problem encountered	

Project	INFINITY
Full Title	IMMERSE. INTERACT. INVESTIGATE
GRANT AGREEMENT ID:	883293
Source of information	https://cordis.europa.eu/project/id/883293
EU contribution	€ 6 866 503,75
Coordinator	AIRBUS DEFENCE AND SPACE SAS 31 Rue Des Cosmonautes Zi Du Palays 31402 Toulouse Cedex
Website:	http://www.astrium.eads.net/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999809265/883293
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 June 2020
End Date	31 May 2023
Description of any problem encountered	

Project	INHERIT
Full Title	INHibitors, Explosives and pRecursor InvesTigation
GRANT AGREEMENT ID:	101021330
Source of information	https://cordis.europa.eu/project/id/101021330
EU contribution	€ 4 882 980,00 against a total cost of: € 5 010 742,50
Coordinator	TOTALFORSVARETS FORSKNINGSINSTITUT Gullfossgatan 6 164 90 Stockholm, Sweden
Website:	http://www.foi.se/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999627875/101021330
Funding Scheme	Innovation Action (IA)
Start Date	1 June 2021
End Date	31 May 2024
Description of any problem encountered	

Project	TRACE
Full Title	Tracking illicit money flows
GRANT AGREEMENT ID:	101022004
Source of information	https://cordis.europa.eu/project/id/101022004
EU contribution	€ 963 875,00
Coordinator	COVENTRY UNIVERSITY Priory Street, CV1 5FB Coventry UK
Website:	http://www.coventry.ac.uk/

Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999612161/101022004
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 July 2021
End Date	30 June 2024
Description of any problem encountered	

Project	ODYSSEUS
Full Title	Preventing, Countering, And Investigating Terrorist Attacks Through Prognostic, Detection, And Forensic Mechanisms For Explosive Precursors
GRANT AGREEMENT ID:	101021857
Source of information	https://cordis.europa.eu/project/id/101021857
EU contribution	€ 4 996 350 against a total costs of: € 5 604 543,75
Coordinator	INSTITUT PO OTBRANA Prof. Tsvetan Lazarov Blvd. 2, 1574 Sofia, BG
Website:	https://odysseus-h2020.eu/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/958304323/101021857
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Aug 2021
End Date	30 Sep 2024
Description of any problem encountered	

Project	CC-DRIVER
Full Title	Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour A Research
GRANT AGREEMENT ID:	883543
Source of information	https://cordis.europa.eu/project/id/883543
EU contribution	€ 4 997 630
Coordinator	TRILATERAL RESEARCH LTD Crown House 72 Hammersmith Road, W14 8TH London, United Kingdom
Website:	http://www.ccdriver-h2020.com/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/923930724/883543
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 May 2020
End Date	30 Apr 2023
Description of any problem encountered	

Project	COSMIC
Full Title	CBRNE Detection in Containers
GRANT AGREEMENT ID:	786945
Source of information	https://cordis.europa.eu/project/id/786945
EU contribution	€ 3 498 867,50
Coordinator	LINGACOM LTD

	10 Hanechoshet Street Ramat Hachayal, 69710 Tel Aviv
Website:	https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c2e7310a&appId=PPGMS
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/937796971/786945
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Oct 2018
End Date	30 Sep 2021
Description of any problem encountered	

Project	INSIKT
Full Title	Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization
GRANT AGREEMENT ID:	767542
Source of information	https://cordis.europa.eu/project/id/767542
EU contribution	€ 1 533 153,13 against a total costs of: € 2 190 218,75
Coordinator	INSIKT INTELLIGENCE S.L Calle Huelva 106, 9-4 08020 Barcelona, ES
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/919371045/767542
Funding Scheme	
Start Date	1 Oct 2017
End Date	30 Mar 2020
Description of any problem encountered	

Project	DAN
Full Title	High-performance, kiosk-solution for forensic darknet analysis to gain cyber threat intelligence for companies and greatly enhance efficiency and capabilities of European investigation authorities
GRANT AGREEMENT ID:	885845
Source of information	https://cordis.europa.eu/project/id/885845/results
EU contribution	50 000 Euro against 71 429 Euro
Coordinator	MH SERVICE GMBH Barthelsmuhlring 24, 76870 Kandel
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/911406569/885845
Funding Scheme	SME Inst Phase 1
Start Date	1 Oct 2019
End Date	31 Mar 2020
Description of any problem encountered	

Project	TITANIUM

Full Title	Tools for the Investigation of Transactions in Underground Markets
GRANT AGREEMENT ID:	740558
Source of information	https://cordis.europa.eu/project/id/740558
EU contribution	€ 4 991 600
Coordinator	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Giefinggasse 4, 1210 Wien,
Website:	http://www.ait.ac.at/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999584128/740558
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 May 2017
End Date	30 Apr 2020
Description of any problem encountered	

Project	FORESIGHT
Full Title	Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments
GRANT AGREEMENT ID:	833673
Source of information	https://cordis.europa.eu/project/id/833673
EU contribution	€ 5 997 018,50 against total costs of: € 7 292 435
Coordinator	KENTRO MELETON ASFALEIAS P Kanellopoulou 4 St 10177 Athina, Gr
Website:	http://www.kemea.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999827307/833673
Funding Scheme	
Start Date	1 Oct 2019
End Date	31 Mar 2023
Description of any problem encountered	

Project	CYBER-TRUST
Full Title	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
GRANT AGREEMENT ID:	786698
Source of information	https://cordis.europa.eu/project/id/786698
EU contribution	€ 2 996 182,50
Coordinator	KENTRO MELETON ASFALEIAS, P Kanellopoulou 4 St 10177 Athina, Gr
Website:	https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bd8ccc07&appId=PPGMS
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999827307/786698
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 May2018
End Date	31 July 2021

Description of any problem encountered	

Project	CyberSec4Europe
Full Title	Cyber Security Network of Competence Centres for Europe Critical Infrastrutures
GRANT AGREEMENT ID:	830929
Source of information	https://cordis.europa.eu/project/id/830929
EU contribution	€ 15 999 981,25
Coordinator	JOHANN WOLFGANG GOETHE-UNIVERSITAET FRANKFURT AM MAIN Theodor W Adorno Platz 1, 60323 Frankfurt Am Main - D
Website:	https://cybercompetencenetwork.eu
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999978724/830929
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Feb 2019
End Date	31 July 2022
Description of any problem encountered	

Project	CONCORDIA
Full Title	Cyber security cOmpeteNCe fOr Research anD InnovAtion
GRANT AGREEMENT ID:	830927
Source of information	https://cordis.europa.eu/project/id/830927
EU contribution	€ 15 998 737,50
Coordinator	UNIVERSITAET DER BUNDESWEHR MUENCHEN Werner Heisenberg Weg 39, 85579 Neubiberg
Website:	http://www.unibw.de/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999630009/830927
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Jan 2019
End Date	31 Dec 2022
Description of any problem encountered	

Project	ECHO
Full Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
GRANT AGREEMENT ID:	830943
Source of information	https://cordis.europa.eu/project/id/830943
EU contribution	€ 15 987 285
Coordinator	ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL Avenue De La Renaissance 30, 1000 Bruxelles
Website:	https://echonetwork.eu/

Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999831575/830943
Funding Scheme	Research and Innovation Action (RIA)
Start Date	1 Feb 2019
End Date	31 Jan 2023
Description of any problem encountered	NOTIONES partner Z&P is in the consortium

Project	TRUST aWARE
Full Title	Enhancing Digital Security, Privacy and TRUST in softWARE
GRANT AGREEMENT ID:	101021377
Source of information	https://cordis.europa.eu/project/id/101021377
EU contribution	€ 4 645 031,25 against a total of: € 5 244 997,50
Coordinator	TREE TECHNOLOGY SA De La Pomarada 76, 33429 Siero ES
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/904959658/101021377
Funding Scheme	Innovation Action (IA)
Start Date	1 June 2021
End Date	31 May 2024
Description of any problem encountered	

Project	SIMARGL
Full Title	Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware
GRANT AGREEMENT ID:	833042
Source of information	https://cordis.europa.eu/project/id/833042
EU contribution	€ 4 984 260 against a total cost of € 6 076 050
Coordinator	FERNUNIVERSITAT IN HAGEN, Universitatsstrasse 47, 58097 Hagen, Germany
Website:	
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999610609/833042
Funding Scheme	Innovation Action (IA)
Start Date	1 May 2019
End Date	30 Apr 2022
Description of any problem encountered	

Project	ADABTS
Full Title	Automatic Detection of abnormal Behaviour and Threats in crowded Spaces
GRANT AGREEMENT ID:	218197
Source of information	https://cordis.europa.eu/project/id/218197/reporting

EU contribution	€ 3 229 034 of a total costs : € 4 523 994
Coordinator	TOTALFORSVARETS FORSKNINGSINSTITUT,
Website:	http://www.foi.se/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999627875/218197
Funding Scheme	CP - Collaborative project (generic)
Start Date	1 Aug 2009
End Date	30 July 2013
Description of any problem encountered	