



NOTIONES

iNteracting netwOrk of iTelligence
and securly practitiOners with
iNdustry and acadEmia actorS



D5.3

Monitoring of EU Research and Horizon Scanning -v2



Project Details

Acronym: **NOTIONES**
 Title: **iNteracting netwOrk of iTelligence and securty 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 ICESA – INTELLIGENCE CULTURE AND STRATEGIC ANALYSIS	ICESA	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:	D5.3
Title:	Monitoring of EU Research and Horizon Scanning -v2
Lead beneficiary:	Z&P
Work package:	WP5
Dissemination level:	PU (Public)
Nature:	Report (RE)
Due date:	31 st October 2022
Submission date:	28th October 2022
Authors:	Giulia Venturi, Maria Ustenko, Z&P; Claudio Testani, Giulia Treossi, APRE
Contributors:	Domenico Frascà, Z&P; Ciro Caterino, EXP.AI; Alessandro Marani, DRI; Janel Cobrun, LAU; Oksana Tsukan, KhNUIA, Andrew Staniforth, SAHER; Alexander Nikolov, SYNYO; Erkuden Rios, Maitena Iardia, TECNA
Reviewers:	Yantsislav Yanakiev, BDI; Alessandro Zanasi (SAB)

Version History:

Date	Version No.	Author	Notes
09/08/2022	0.1	Giulia Venturi, Maria Ustenko (Z&P); Janel Cobrun (LAU)	Initial version with introduction and ToC draft + inputs from T6.1 by LAU (matrix from both WGs)
27/09/2022	0.2	Giulia Venturi, Maria Ustenko (Z&P); Claudio Testani, Giulia Trossi (APRE)	Section 3 (results of monitoring of EU research projects)
28/09/2022	0.3	Domenico Frascà (Z&P)	Annex I (Report about EU framework on AI)
29/09/2022	0.4	Ciro Caterino (EXP.AI)	Contribution in section 4 (NLP innovation by AIDA and ANITA projects)
04/10/2022	0.5	Giulia Venturi (Z&P)	Section 2 (results of horizon scanning)
04/10/2022	0.51	Alessandro Marani (DRI)	Annex II (relationship between LEAs and commercial actors)
06/10/2022	0.6	Oksana Tsukan (KhNUIA)	Annexes III and IV (Trustworthiness of the AI, AlaaS)
11/10/2022	0.7	Giulia Venturi (Z&P)	Section 4 (WP6 follow-up), Section 5 (Main Findings), Conclusions

Date	Version No.	Author	Notes
11/10/2022	0.71	Maria Ustenko (Z&P)	Contribution in section 4 (Face Recognition, Betaface)
11/10/2022	0.72	Erkuden Rios, Maitena Ilardia (TECNA)	Contribution in section 3
14/10/2022	0.73	Andrew Staniforth (SAHER), Giulia Venturi (Z&P)	Annex V (P300)
17/10/2022	0.8	Giulia Venturi (Z&P)	Update of Section 5 (Main Findings) and Conclusions
25/10/2022	0.9	Yantsislav Yanakiev (BDI), Alexander Nikolov (SYNYO), Alessandro Zanasi (SAB)	Review by BDI, review by SAB, contribution by SYNYO in section 4
25/10/2022	1.0	Giulia Venturi, Maria Ustenko (Z&P)	Finalized version


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

Table of Content

Project Details.....	2
Deliverable Details.....	4
Table of Content.....	6
List of Figures.....	7
List of Tables.....	8
Acronyms.....	9
Executive Summary.....	10
1. Introduction.....	11
1.1 Structure of the document.....	12
2. Research monitoring through Horizon Scanning.....	13
3. Research monitoring on EU projects.....	23
3.1 Dark Web monitoring.....	24
3.2 Intelligence analysis phase.....	25
3.3 Secure Data Sharing.....	39
3.4 Cybersecurity and Cybercrime.....	41
3.5 Artificial Intelligence (AI).....	49
3.6 Technology innovation.....	57
4. Follow-up of recommendations from WP6.....	72
4.1 T6.1 recommendations.....	72
4.2 D6.7 recommendations.....	85
5. Main findings.....	87
6. Conclusions and next steps.....	92
References.....	94
Annex I EU framework on Artificial Intelligence.....	96
Annex II The relationship between LEAs and commercial actors.....	104
Annex III Trustworthiness of the AI.....	113
Annex IV Artificial Intelligence as a Service.....	124
Annex V P300 technology for HUMINT.....	135

List of Figures

Figure 1: Time diagram of the second run of innovation monitoring in WP5.....	11
Figure 2: Diagram of the horizon scanning research.....	14
Figure 3: T5.2 Process description.....	23
Figure 4: Text Analysis Flow	80
Figure 5: ANITA Validation Flow	81
Figure 6: New Knowledge Extraction	82
Figure 7 - Main results: INSPECTr project.....	87
Figure 8 - Main results: i-LEAD project.....	88
Figure 9 - Main results: LAW-GAME project.....	89
Figure 10 - Main results: cyber ranges	90
Figure 11 - Main results: P300 technology	91

List of Tables

Table 1 Selected projects for Dark Web	25
Table 2 Selected projects for Intelligence	25
Table 3 Results of the PREVISION project	27
Table 4 Results of the INFINITY project	28
Table 5 Results of CYBER-TRUST project	29
Table 6 Results of EU-HYBNET project	31
Table 7 Results of ROXANNE project	34
Table 8 Results of CREST project	36
Table 9 Results of CTCMR project	38
Table 10 Selected projects for Secure Data Sharing.....	39
Table 11 Results of INSPECTr project	40
Table 12 Results of I-LEAD project.....	41
Table 13 Selected projects for Cybersecurity and Cybercrime	41
Table 14 Results of CONCORDIA project	42
Table 15 Selected projects for Artificial Intelligence	49
Table 16 Results of TAILOR project	55
Table 17 Selected projects for technology innovation.....	57
Table 18 Selected projects for technology innovation.....	58
Table 19 Results of CONNEXIONS project	59
Table 20 Results of PROACTIVE project.....	64
Table 21 Results of MEDEA project	67
Table 22 Results of DARLENE project	68
Table 23 Results of TRAPEZE projects	69
Table 24 Results of TechEthos project	71
Table 25 Research projects and technologies/tools voted by WG1 and WG2	73
Table 26 Cybercrime Taxonomy comparison before and after changes.....	76
Table 27 Terrorism Taxonomy comparison before and after changes	77

Acronyms

AI HLEG	High-Level Expert Group on Artificial Intelligence
AIA	Artificial Intelligence Act
AlaaS	Artificial Intelligence as a Service
APCO	Association of Chief Police Officers of England, Wales and Northern Ireland
APWG	Anti-Phishing Work Group
CEPOL	European Union Agency for Law Enforcement Training
CSA	Coordination and Support Action
DAAI	Defence Applications of Artificial Intelligence
EC	European Commission
EC	European Commission
EC3	European Cybercrime Centre
ECSO	European CyberSecurity Organization
EEG	electroencephalography
E-FCR	ECHO Federated Cyber Range
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENFSI	European Network for Forensic Science Institutes
ENISA	European Union Agency for Cybersecurity
EP	European Parliament
FRT	Facial Recognition Technology
GDPR	General Data Protection Regulation
HE	Horizon Europe
LEA	Law Enforcement Agency
MERMER	Memory and Encoding Related Multifaceted Electroencephalographic Response
NER	Name entity recognition
NLP	Natural Language Processing
NRRP	National Recovery and Resilience Plan
PMC	Private Military Company
SWIDE	Scientific Working Group on Digital Evidence
TAM	Text Analysis Module
TF-IDF	term frequency – Inverse document frequency
ToR	The Onion Router
TTC	Trade and Technology Council
UAE	United Arab Emirates
WP	Work Package

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 M13 and M14 since the beginning of the project (second 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. Datasets were explored searching for publications of relevance for the third and fourth NOTIONES *focus areas*.

Section 3 reports on the research activities carried out in task T5.2 “*Research monitoring on EU projects*” through cascade refinement stages of research, to identify the most interesting projects in terms of relevance for the NOTIONES *focus areas*.

Section 4 presents the results of the follow-up of the recommendations delivered in WP3 and WP6.

Section 4.1 reports on the projects and technologies voted as relevant by practitioners in the first round of the NOTIONES Working Groups (T6.1). Sub-section 4.1.1 especially contains the information found about the research projects that rose the interest of the practitioners, based on a direct contact with the coordinators and partners in the consortia of the projects themselves.

Section 4.2 presents the thematic deepening performed on selected research topics recommended for further investigation in D6.7, reported at the end of the document as annexes:

- EU framework on Artificial Intelligence (Annex I)
- The relationship between LEAs and commercial actors (Annex II)
- Trustworthiness of the AI (Annex III)
- Artificial Intelligence as a Service (Annex IV)
- P300 technology (Annex V)

Section 5 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 research projects and technologies are presented and their possible exploitation in NOTIONES is proposed:

- INSPECTr project;
- I-LEAD project;
- LAW-GAME project;
- Cyber ranges;
- P300 technology.

Section 6 contains conclusive considerations and next steps.

Finally, the five annexes to this deliverable provide the results of the thematic deepening performed in the second run of WP5 about selected topics.

1. Introduction

NOTIONES (iNteracting netWOrk of iTelligence 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.

NOTIONES 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 **innovation 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 second run of tasks T5.2 and T5.3 of WP5, which performed the research monitoring activities during M13 and M14, as depicted in Figure 1.



Figure 1: Time diagram of the second 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 and 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 D5.12 “*Monitoring of Emerging terrorist threats -v2*”.

WP5 also took responsibility of the follow-up of recommendations provided by previous tasks and Work Packages, providing updated information on:

- research projects and technologies considered relevant by the NOTIONES practitioners in WP6;
- topics tackled in WP3 that needed further investigation.

1.1 Structure of the document

Section 1 introduced 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*”.

Section 3 reports on the research activities carried out in task T5.2 “*Research monitoring on EU projects*”.

Section 4 presents the results of the follow-up of the recommendations delivered in WP3 and WP6. Section 4.1 reports on the projects and technologies voted as relevant by practitioners in the first round of the NOTIONES Working Groups. Section 4.2 presents the thematic deepening performed on selected research topics recommended for further investigation in D6.7 (reported at the end of the document as annexes).

Section 5 contains a summary of the most relevant findings of both tasks T5.2 and T5.3.

Section 6 contains conclusive considerations and next steps.

Annexes to this deliverable provide the results of the thematic deepening performed in the second run of WP5 about selected topics, as follows:

- Annex I describes the EU framework on Artificial Intelligence in which AI solutions need to frame;
- Annex II discusses about the relationship between LEAs and commercial actors;
- Annex III gives light about the requirements of Trustworthiness of the AI;
- Annex IV explains the paradigm of Artificial Intelligence as a Service;
- Annex V details the P300 technology for HUMINT.

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 and 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.

For the second run of task T5.3, Horizon Scanning was performed by researching technologies through the analysis of free online scholar and patent databanks.

The methodology adopted for task T5.3 originates from the methodology delivered in D5.1 "*Methodology for innovation monitoring*". The main data source used was TheLens [1], 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. Apart from TheLens, open web and CORDIS [2] were also exploited. The datasets were primarily explored with the online statistical analysis tool of TheLens.

The research was performed by Mrs. Giulia Venturi (Orcid ID: 0000-0003-0445-2613) and Ms. Maria Ustenko (Orcid ID: 0000-0002-6506-7607) of Consortium partner Z&P.

Mrs. Venturi 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.

Ms. Ustenko 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.

With regard to the issues encountered and search features, the explanations provided in the first version of this deliverable (D5.2) remain valid.

In the next subsections, the results of the horizon scanning activities performed in the second run of WP5 are presented.

The focus areas tackled in this run of the horizon scanning task are respectively the third and fourth most voted focus areas enlisted in WP2 and ranked in WP7, namely:

- Technological Solutions to Secure Data Sharing and Dissemination (internally and externally);
- Improvements and Innovations to Various Intelligence Related Training.

It is worth reminding that the first and second focus areas – which are the subject of the first NOTIONES Working Groups - were investigated in the first run of the innovation monitoring task.

The horizon scanning performed in the second run of task T5.2 took as a starting point the NOTIONES focus area “Improvements and Innovations to Various Intelligence Related Training” and proceeded in a pure exploratory way, through wide-ranging research.

The diagram of the research is shown in Figure 2, to assist the reader as he/she progresses in reading the report, which appears jingly at times due to its exploratory nature.

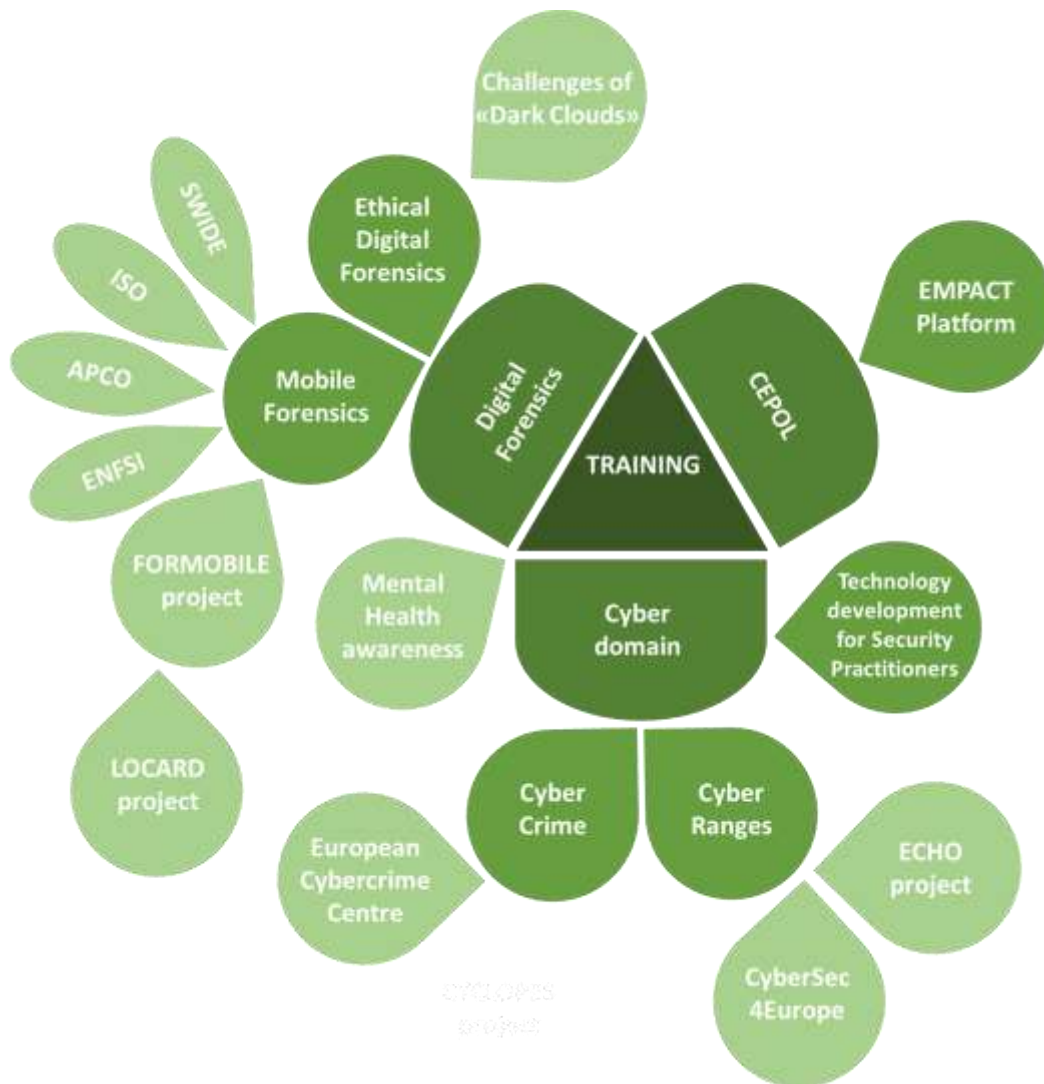


Figure 2: Diagram of the horizon scanning research

The very first search on the online scholar database *TheLens* with keyword “Training” AND “Law Enforcement” in all search fields, with date range limitation to years 2020-2022, in the European Jurisdictions, with subject matter “Law Enforcement”, led to 59 results, described below.

Mental Health:

A relevant number of the results referred to training guidelines for Law Enforcement addressing **mental health** issues, such as publications about the enhancement of intellectual disability awareness amongst law enforcement officers [3] [4] or about the need to increase mental health literacy in law enforcement [5] [6], or about the need to facilitate the referral of persons with suspected mental illnesses to mental health services by law enforcement officers [7].

Ethical Digital Forensics:

Another publication reported about a framework for ethical digital forensics investigations called PRECEPT (Privacy-Respecting EthiCal framework) [8]. The paper “*argues the need for a practical, ethically grounded approach to digital forensic investigations, one that acknowledges and respects the privacy rights of individuals and the intellectual capital disclosure rights of organizations, as well as acknowledging the needs of law enforcement*”, deriving a set of ethical guidelines, and then mapping these onto a forensics investigation framework. The recommendations gathered in the paper are consolidated into the following set of 10 ethical principles:

- E1 Delineate Remit: Commence by carefully delineating the remit of the investigation
- E2 Respect the privacy of the subject: The privacy of the subject should be protected by only investigating topics identified as being of interest to the investigation. In particular, examination scope should be identified before the investigation proceeds.
- E3 Only investigate other parties if there is evidence of their involvement: The privacy of third parties should be protected by only investigating them if there is evidence that they have been implicated in the topic of the investigation.
- E4 Exclude private information: During investigation, bookmark private information that is irrelevant to the investigation so that it is not included in any report. Examples are personal credit card numbers, personal passport numbers, and national insurance numbers.
- E5 Document all actions: Document all data that was examined, judged private and irrelevant, and relevant to the investigation
- E6 Facilitate audits: Facilitate post-investigation scrutiny.
- E7 Report all investigative activities: When the investigation is concluded, the report should include details of exactly what was examined, who was included in the investigation, which devices were examined (and who they belonged to), how data was classified as relevant (to be reported), confidential (only to be reported if the court so orders), irrelevant (not to be divulged) and how the data was preserved to prevent any alteration.
- E8 Be transparent about the extent of the investigation, and the gathered information: Subjects, and their counsel, have to be given the right to know what data was processed and how it was processed.
- E9 Investigators should undergo regular training: Investigators should undergo frequent proficiency training and testing.
- E10 Information’s Integrity and Confidentiality should be maintained: Investigators should carry out investigations lawfully and with integrity, and confidentiality.
- E11 Consideration for the wellbeing of investigators.

The authors report that the first four ethical principles proposed do not align with current investigative guidelines in the UK, which recommend to exhaustively investigate, comprehensively record all information, investigate all relevant related parties, and record also sensitive material while marking it as such.

In any case, the interest of NOTIONES in this paper goes beyond such ethical guidelines, that are very important.

In fact, the paper also states that *“the difficulties forensic investigators face is clear. They walk the tightrope between protecting and violating citizens’ privacy during their labors. This is made more difficult by a lack of agreement about the definition of privacy, on the one hand, and the ability to know when our privacy has been violated, on the other. Governments, too, face a conundrum. They react to perceived threats by implementing ever more complex and covert surveillance, and enact privacy-invasive legislation. Citizens react by adopting ever more sophisticated privacy-protecting technologies, preventing government surveillance”*.

Indeed, as the capability of digital investigations to uncover evidence is increasing, mechanisms designed specifically to preserve privacy are doing the same, countering the efforts of forensics investigators. These include encryption, full disk encryption using tools such as VeraCrypt or Bitlocker, secure network communication using Virtual Private Networks, Secure Processors, homomorphic encryption and anonymous routing using TOR.

The risk is that improvements in cyber security, privacy-preserving tools and encryption could lead towards a future *“information blackout”* for those who carry out digital forensics investigations. The paper reports the following evidence that this is already happening, referred to as *“dark clouds”* in literature:

- a) First responders start to avoid simply ‘pulling the plug’ (thereby losing provided encryption keys) and make use of live imaging techniques rather than the more forensically sound static techniques;
- b) The encryption techniques used in consumer devices (such as smartphones) are now sufficiently strong to prevent law enforcement access without the cooperation of the manufacturer. However, other cases demonstrate that defects in the implementation of the encryption technology could still be exploited to allow access.
- c) The VPN market has grown dramatically, predicting the future widespread adoption of communications encryption by the average citizen.
- d) The increase in the number of ToR (The Onion Router) nodes also reveals an uptake in privacy-preserving technologies.

Thus, *“security services and law enforcement are aware of the way these privacy-preserving technologies are starting to prevent them from gathering digital evidence. Some governments and law enforcement agencies have responded by demanding access to privately held information and the ability to decrypt information.”*

Law enforcement is also increasingly demanding that software companies insert *“back doors”* (secret entrances designed into the system), but, unfortunately, they do not remain secret for long: to the contrary, they are likely to offer an entry to hackers.

Furthermore, *“it is understood that those who engage in criminal or terrorist activities are likely to be aware of the security services’ attempts to monitor them, and so use advanced (or offline) techniques to hide their communications. Therefore, those with the least to hide are also those who are the most surveilled, leaving the security services with largely the same problems as before”*.

The paper also enlists other anti-forensic techniques, including: artifact-wiping via file-wiping, artifact-wiping via disk-wiping, artifact-wiping via log-wiping, data-hiding via vault app, data-hiding via proxy server, data-hiding via IP address-spoofing, trail obfuscation via private browsing, and trail obfuscation via e-mail encryption.

The authors note that *“Forensics investigators experience difficulties in understanding how to address these issues whilst still conducting their investigations and safeguarding communities from crime and terrorism. It is unsurprising that they may consider the integration of ethical considerations into their investigations a step too far, given the challenges these dark clouds already constitute”*. But still, law enforcement must not ignore ethical constraints.

Further research and comments on this topic:

A publication about Dutch criminal court cases [9] was found, which investigates to what extent end-to-end encryption (E2EE) hampers authorities prosecuting criminals who rely on encrypted communication - ranging from drug syndicates to child sexual abuse material (CSAM) platforms. The authors analysed public court data from the Netherlands to show to what extent law enforcement agencies and the public prosecution service are impacted by the use of E2EE in bringing cases to court and their outcome, especially with regard to the use of Pretty Good Privacy (PGP, an encryption program that provides cryptographic privacy and authentication for data communication) and WhatsApp. The results showed that *“Dutch law enforcement appears to be as successful in prosecuting offenders who rely on encrypted communication as those who do not”*, for cases that reach court. Anyway, it should be noted that the data does not permit to draw conclusions on the effect of E2EE on criminal investigations, but only on investigations that led to a court case.

It would be relevant to understand the impact of such technologies on investigations within the NOTIONES network.

Mobile Forensics:

A very interesting work was retrieved, on Law enforcement educational challenges for **mobile forensics** [10] by Humphries *et al.* The abstract of the paper states: *“Training, tools, and standards are important foundations of mobile forensics. This work focuses on existing curricula and courses in the domain of mobile forensics. In order to identify courses in areas of computing where mobile forensics may be offered, this research utilises open source information gathering, in addition to questionnaire and interviews, to capture additional information and the views and experiences of educators and/or trainers. This research finds that current education and training offerings mainly include topics regarding acquisition of mobile devices and analysis of the acquired data. Current education and training do not cover the areas of a complete mobile forensic investigation, from crime scene to court. In addition, trainer opinions on skills shortages include the lack of basic knowledge, generic skills in forensics and investigation, lack of skilled practitioners, and necessary mindsets to critically think, investigate and avoid dependency on Digital Forensic software”*.

Even more relevant to NOTIONES, the paper reports about the debate surrounding standardisation and certification within digital forensics. Several accreditation programs, processes, standards, and best practices were presented in the past, and best Practices have been identified: these include for example, the Good Practice Guideline by the Association of Chief Police Officers of England, Wales and Northern Ireland (APCO) [11], the ISO/IEC 17025 Forensic Lab Accreditation Process [12], and Best practice manual for the forensic examination of digital technology by the European Network for Forensic Science Institutes (ENFSI) [13]. In addition to this, best practices regarding mobile forensic investigations were also provided by the Scientific Working Group on Digital Evidence (SWIDE, under the National Institute of Standards and Technology of the USA) [14]. The authors note that Law Enforcement Agencies (LEAs) also implement several Standard Operating Procedures (SOPs) adding another level of standardisation to investigations. In their opinion, *“although there is an abundance of literature on forensic investigation processes, and several standards and best practice guidelines, practitioners have experienced mixed approaches with little clarity, which have led to a lack of internationally accepted standards within the field of digital forensics and mobile forensics for several years”*.

The work included literature review, open information gathering, and interviews with practitioners and trainers, and it found that current courses and training in mobile forensics are not covering the crime scene, but are covering mainly acquisition and analysis. The trainers feel they cover analysis the most, but course

descriptors yield acquisition as the most included category. The inquiry/investigation may not be covered in depth, and the training/education for prosecution and court (decision phase) is missing.

Further research and comments on this topic:

The research conducted in this study by Humphries *et al.* was used to inform the design of the FORMOBILE Mobile Forensic Curriculum for law enforcement.

within the **FORMOBILE** (From Mobile Phones to Court - A complete FOREnsic investigation chain targeting MOBILE devices) project, which has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800. The project ended in April 2022, and delivered a complete end-to-end forensic investigation chain for mobile devices. Methods were developed and implemented to cover the forensic acquisition of data from mobile devices, plus the decoding and analysis of the data as well as the presentation of the evidence. Many of the FORMOBILE's work products are available on its website¹. NOTIONES practitioners may be interested in such innovation and related training.



A sister project of FORMOBILE is **LOCARD** (Lawful evidence collecting and continuity platform development), which received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no. 832735. LOCARD aims to procure a comprehensive platform that permits the storage of digital evidence data and ensures appropriate chain custody in juridical work. It employs a "Trusted Execution Environment" to guarantee privacy and provide access to a range of digital evidence. LOCARD developed a next generation platform to process digital evidence through blockchain technology and generate mutual recognition of judicial decisions among the EU, with all the related training material. The project ended in July 2022 and many of its work products are available on its website².

CEPOL and EMPACT:

The original research on the *TheLens* database returned also an interesting publication was found about the role of law enforcement training in combatting illicit tobacco trade [15]. The authors refer multiple times to the **CEPOL** (European Union Agency for Law Enforcement Training) training activities [16], praising its role in providing access to a full range of learning resources, including online learning modules, platforms of communities of practice, webinar resources and access to the repository of professional e-Journals and e-books.



NOTIONES practitioners are probably well aware of such Agency. In any case, for those who are not familiar with it, it is important to remind that to participate in online CEPOL training activities, law enforcement officials must be registered users of CEPOL's online learning platform (LEEd) To apply to residential or other type of CEPOL training activities, law enforcement officials should visit the agency's website. Courses are in English language, but also modules in French language have been recently added to the platform. A dedicated

¹<https://formobile-project.eu>

² <https://locard.eu>

section of the training courses addresses the topic of Law Enforcement cooperation, information exchange and interoperability³, with many subcategories which include Intelligence analysis.

The publications found also mention the **EMPACT platform** (European Multidisciplinary Platform Against Criminal Threats) [17], which introduces an integrated approach to EU internal security, involving measures that range from external border controls, police, customs and judicial cooperation to information management, innovation, training, prevention and the external dimension of internal security, as well as public-private partnerships where appropriate.



Cybercrime:

The search about training also led to results related to **cybercrime awareness** for law enforcement officers. One of the papers reviews in-depth, common, cybersecurity countermeasures including legislation, law enforcement, hands-on training, and education among others, with focus on phishing attacks [18]. The paper reports governmental initiatives on the topic, for example it is reported that *“the United Kingdom (UK) strengthened its legal system against cybercrimes, including fraud and identity theft, by introducing a new law in 2006 called the Fraud Act. The act increased prison sentences (up to ten-years) for online fraud offences that included phishing. The government also set up Action Fraud, a website dedicated to national fraud and cybercrime where users can find educational materials on different cybercrimes and have a forum for reporting any suspicious activities”*. The authors state that many other countries have enacted similar laws for combatting phishing and other cybercrimes. According to the references sources, legislation should be designed to provide large-scale damage against individual phishers or secondary liability against Internet Service Providers (ISPs) in hopes that ISPs will be motivated to play their role in fighting phishing under the auspices of intellectual property or unfair competition laws. However, cybercrime is mostly done cross-border and many phishing attacks have a short life-span, so that the two main challenges are locating the phisher and obtaining jurisdiction to enforce the law. The authors conclude stating the following: *“It can be seen that according to the International APWG (Anti-Phishing Work Group), many phishing attacks originate from countries that have very lenient or weak cyber laws. Extraditing such criminals would thus be virtually impossible when such treaties do not exist between foreign states. Countries that do not have cybercrime laws need to act and enact legislation that will criminalize these activities. A globally harmonized policy will be required in order to have a uniform definition of what amounts to cybercrime which can be implemented across all countries with similar legislations. Extradition treaties that can be enforced through law enforcement agents such as the International Police organization (INTERPOL) should then be encouraged among member countries. It is quite obvious that extradition is time consuming, not a cost-effective process, and may require a lengthy court process in the native countries (even on crimes where the suspects have physical addresses or business), yet nonetheless, is a necessary first step toward combating this menace at a global scale. Information sharing among countries is also critical to fighting cyber criminals”*.

It should be noted that in the EU cybercrime is defined as consisting of criminal acts committed online by using electronic communications networks and information systems. The EU has implemented laws and supports operational cooperation through non-legislative actions and funding [19]. Cybercrime is a borderless issue that can be classified in three broad definitions:

- crimes specific to the internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts)
- online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code

³ <https://www.cepol.europa.eu/education-training/what-we-teach/law-enforcement-cooperation-information>

- illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia

The **European Cybercrime Centre (EC3)**, established in 2013 by Europol, acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise offer operational, strategic, analytical and forensic support to Member States' investigations across law enforcement and the judiciary. At the level of operations, EC3 focuses on the following types of cybercrimes: cyber-dependent crime, child sexual exploitation and payment fraud. The support provided extends also to tackling criminality on the Dark Web and alternative platforms [20].



Cybersecurity:

Another result of the search referred to **Cybersecurity** and related training, in particular the emerging relevance of **Cyber Ranges** [21]. The publication states that *“For the successful prevention and mitigation of sophisticated cyber-attacks and minimization of cyberthreat risks, engagement in training activities is vital. Cyber ranges are environments offering tools and services to support cybersecurity and forensic simulation and training experience. Therefore, the design and development of cyber ranges have become a necessity for many governmental bodies and organizations such as law enforcement and defence agencies. [...] a cyber range allows the reproduction of IT and/or OT systems execution in a simulated environment (composed by both virtual and physical components)”*.

According to the European CyberSecurity Organization (ECSO), *“a cyber range is a **platform for the development, delivery and use of interactive simulation environments**. A simulation environment is a representation of an organisation’s ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases”*. [22]

Further comments on this topic:

It should be noted that Cyber Ranges are recognized as a key part of the EU strategy also for Defence: The Permanent Structured Cooperation (PESCO) has an ongoing project about Cyber Ranges Federations. The primary objective is to enhance the European Cyber Ranges capability by federating existing national Cyber Ranges into a larger cluster with more capacity and unique services. This correspondingly enables to share and pool the capabilities and improve the quality of cyber trainings, exercises as well as using the federation for cyber-related research and development purposes.

The NOTIONES network is already aware of the importance of cyber ranges in the training related to cybersecurity, because NOTIONES has started a close collaboration with the ECHO project. ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations) is a research project which has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement no 830943. The project organized the ECHO Federated Cyber Range (E-FCR) demonstration workshop on 21st September 2022 and some of the partners on NOTIONES joined it. The E-FCR is a multipurpose virtualization environment for hands-on cyberskills development and realistic simulations for improved system



assurance. It is a virtual environment used as development and demonstration of technology roadmaps and deliver of specific instances of the cyberskills training curricula.

Another project that deserves to be mentioned at this point CYCLOPES (European Network Of Practitioners Fighting Cybercrime), which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 101021669. CYCLOPES aim



is to establish a network of different stakeholders across Europe, with a wide range of experience in the field of fighting cybercrime. The network, in addition to identifying capability gaps and requirements and sharing best practices, will focus on the ongoing dialogue with industries and academia who are delivering products and conducting

research on solutions that help fight cybercrime. The consistent cooperation between LEAs, industry and academia will not only improve the possibilities of practitioners fighting cybercrime but will contribute to the development of European markets.

Another initiative on this topic is CyberSec4Europe, funded by the European Union under the H2020 Programme Grant Agreement No. 830929. This is a research and innovation pilot for the planned European Cybersecurity Competence Centre in Bucharest and the Network of cybersecurity expertise. As part of its activities, CyberSec4Europe federated



a commercial Amazon AWS cloud component into a cyber range and creating a federation network for end users joining a cyber exercise. In the demonstration, network traffic was tunnelled in the federation network through the public Internet between the participants' commissioned workstations and exercise network, and between the exercise network and Amazon AWS. The demonstrated open-source software-only solution performed with high throughput, low latency and low CPU usage, as monitored by the cyber exercise conductor from the exercise network. The tested solution is estimated to be production-ready to be used in cross-border cyber exercises. The benefit of software-only open-source solution is that no investment in hardware or software licenses is required to establish a cyber range technical federation. However, a skilled workforce to plan and implement a federation network is required [23].

More on Cybersecurity:

Given the relevance of cybersecurity training for Law Enforcement purposes, a new search on the online scholar database *TheLens* was performed with keyword “*cybersecurity*” in search fields title and abstract, with date range limitation to years 2020-2022, in the European Jurisdictions, with subject matter “*Law Enforcement*”, which led to 8 results – not all relevant for NOTIONES.

The only relevant publication found was again about cyber ranges [24], a chapter of the book “*Technology Development for Security Practitioners*”, part of the “*Security Informatics and Law Enforcement*” (SILE) book series. The primary objective of this book series is to explore contemporary issues related to law enforcement agencies, security services and industries dealing with security related challenges (e.g., government organizations, financial sector insurance companies and internet service providers) from an engineering and computer science perspective. Each book in the series provides a handbook style practical guide to one of the following security challenges:



- Cyber Crime - Focuses on new and evolving forms of crimes. Books describe the current status of cybercrime and cyber terrorism developments, security requirements and practices.

- Big Data Analytics, Situational Awareness and OSINT- Provides unique insight for computer scientists as well as practitioners in security and policing domains on big data possibilities and challenges for the security domain, current and best practices as well as recommendations.
- Serious Games – Provides an introduction into the use of serious games for training in the security domain, including advise for designers/programmers, trainers and strategic decision makers.
- Social Media in Crisis Management – explores how social media enables citizens to empower themselves during a crisis, from terrorism, public disorder, and natural disasters
- Law enforcement, Counterterrorism, and Anti-Trafficking – Presents tools from those designing the computing and engineering techniques, architecture or policies related to applications confronting radicalisation, terrorism, and trafficking.

The books pertain to engineers working in law enforcement and researchers who are researching on capabilities of LEAs, though the series is truly multidisciplinary. NOTIONES practitioners may be interested in this book series.

3. Research monitoring on EU projects

A search on the European Community CORDIS (Community Research and Development Information Service) Platform⁴ was performed, with regard to the most promising research projects in the field of intelligence and security. To this purpose, the search performed during the first run of Task T5.2 was repeated and enlarged, to include newly-funded actions.

Following the indication of the deliverable D5.1 “*Methodology for Innovation Monitoring*”, the activities of the task T5.2 have been focused on a further 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.

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, as already done during the previous run of task T5.2.

While in the previous scanning round the date range was set for projects starting from 2009, for this second updated analysis the spotlight was set on projects starting from 2018, highlighting newly financed projects. Such search resulted in a list of 75 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, 60 projects were selected out of the initial 75. These were further investigated by examining in deep the projects’ objectives and results. 41 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.

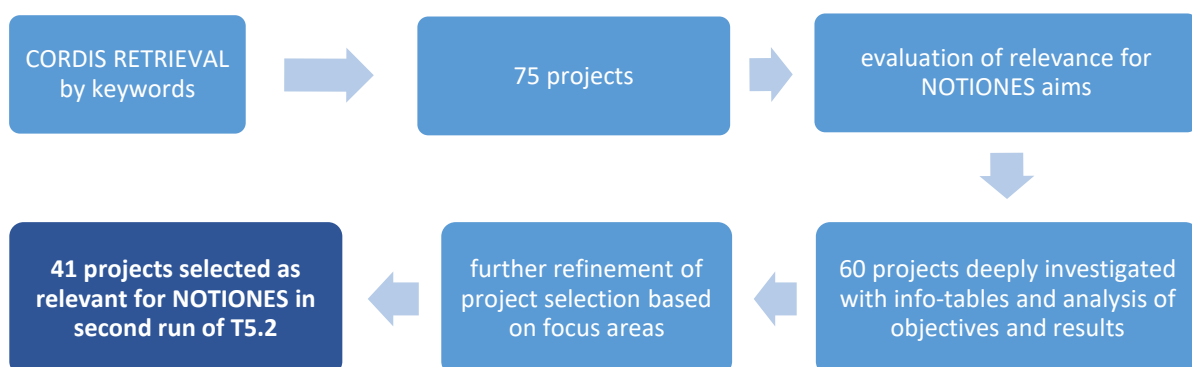


Figure 3: T5.2 Process description

The research was performed by Ms. Giulia Treossi and by Mr. Claudio Testani (Orcid ID: 0000-0002-5312-6016, Hi=13) of Consortium partner APRE, and Dr. Erkuden Rios (Orcid ID:0000 0001 5541 1091) from partner TECNA.

⁴ <https://cordis.europa.eu>

Ms. Treossi holds a Bachelor’s degree in Political Science and International Relations and Master’s degree in International Relations (University of Rome La Sapienza). Moreover, she obtained a Master of Expertise in EU Project Management and Internationalization of Enterprises (Italian Society for International Organisation, SIOI) . She is member of APRE’s Thematic Theme – Cluster 3 (Civil Security for Society).

Mr. Testani 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, he 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.

Dr. Erkuden Rios holds a Mater’s degree in Telecommunications Engineering (Basque Country University, Bilbao, Spain) and is the current coordinator of NOTIONES project, and AI4CYBER Horizon Europe project on AI for Cybersecurity reinforcement. She is senior researcher at Tecnalia for more than 18 years and she has coordinated and worked in multiple EU-funded research projects on cybersecurity.

In the next subsections, the results of the research project monitoring activities performed in the second run of WP5 are presented.

As already described, by replicating the research through the CORDIS Database 75 projects were initially retrieved from the CORDIS database, also comprehensive of the already outlined results from the 1st round of search performed for deliverable D5.2. Of these, 60 projects survived the first selection refinement. Starting from these 60, a total of 41 projects were found to have interesting results for NOTIONES, of which 29 projects were not included in the 1st run of search. They are described in different subsections, based on their main research topic/technological area:

- focus area *“Various challenges in monitoring and collecting data from the dark web”* (two projects found in 1st run);
- focus area *“Technological needs, solutions, and improvements to the intelligence analysis phase of the Intelligence cycle”* (four projects found in 1st run, six projects found in the 2nd run);
- focus area *“Technological Solutions to Secure Data Sharing and Dissemination (internally and externally)”* (two projects found in the 2nd run);
- focus area *“cybersecurity and cybercrime”* (two projects found in 1st run, four projects found in the 2nd run);
- focus area *“Artificial Intelligence”* (seven projects found in the 2nd run);
- *other technological innovation areas - including platforms, CBRNE tools, training for LEAs etc. (two projects found in 1st run, ten projects found in the 2nd run).*

3.1 Dark Web monitoring

In the previous deliverable (D5.2) 2 projects were found to have interesting results in terms of relevance with the NOTIONES focus area *“Various challenges in monitoring and collecting data from the dark web”*. The table below enlists these projects:

acronym	title	start-end year	Mapped at
TITANIUM	Tools for the Investigation of Transactions in Underground Markets	2017-2020	1 st search round

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	1 st search round
-----	--	-----------	------------------------------

Table 1 Selected projects for Dark Web

Further search found no other relevant projects on this topic.

No updates were found for project DAN, while for project TITANIUM some interesting updates and results achieved were found, in particular two of its work products appear to be of significant relevance for NOTIONES:

The first is the TITANIUM deliverable "[Report on data sharing and provenance tracking models](#)", which may be interesting with respect to the NOTIONES focus area "*Technological Solutions to Secure Data Sharing and Dissemination (internally and externally)*".

The second is the TITANIUM deliverable "[Training plan](#)", which may be interesting with respect to the NOTIONES focus area "*Improvements and Innovations to Various Intelligence Related Training*".

3.2 Intelligence analysis phase

In the previous deliverable (D5.2) four projects were found to have interesting results in terms of relevance with the NOTIONES focus area "*Technological needs, solutions, and improvements to the intelligence analysis phase of the Intelligence cycle*".

By replicating the mapping on CORDIS Database, further six interesting projects have been selected and added. The table below enlists these projects:

acronym	title	start-end year	Mapped at
PREVISION	Prediction and Visual Intelligence for Security Information	2019-2021	1 st search round
INFINITY	IMMERSE. INTERACT. INVESTIGATE	2020-2023	1 st search round
TRACE	Tracking illicit money flows	2021-2024	1 st search round
CYBER-TRUST	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things	2018-2021	1 st search round
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats	2021-2025	2 nd search round
LINSEC	The Logic of Informal Security Cooperation: Counterterrorism Intelligence-sharing in Europe	2020-2022	2 nd search round
ROXANNE	Real time network, text, and speaker analytics for combating organized crime	2019-2022	2 nd search round
NESTOR	aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders	2021-2023	2 nd search round
CREST	Fighting Crime and TerrorisM with an IoT-enabled Autonomous Platform based on an Ecosystem of Advanced IntelligEnce, Operations, and InveStigation Technologies	2019-2023	2 nd search round
CTCMR	Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies	2016-2021	2 nd search round

Table 2 Selected projects for Intelligence

Below, the objectives and main results of these projects are reported. More specifically, an in-depth analysis of the newly mapped projects - 2nd search round - has been provided, while for the already mapped projects - 1st search round - the main focus was set on the latest updates and results achieved after the first round of mapping.

No updates were found for project TRACE.

PREVISION

Project	PREVISION
Full Title	Prediction and Visual Intelligence for Security Information
GRANT AGREEMENT ID:	833115
Source of information	https://cordis.europa.eu/project/id/833115
Call for Proposal	H2020-SU-SEC-2018
EU contribution	€ 9 040 230,00
Coordinator	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS Patisson 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 project was included in deliverable D5.2 and ended in 2021.

The EU-funded PREVISION project aimed at providing law enforcement agencies with advanced, almost-real-time, analytical support for multiple Big Data streams (coming from various data sources). The project built dynamic and self-learning knowledge graphs that helps investigators becoming more aware in these fields and better address hybrid security threats, i.e. threats that combine physical and cyber-attacks. The project organized 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 was to empower the analysts and investigators of LEAs with tools and solutions not commercially available yet, 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 was 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 advances on object detection and tracking by investigating a novel hybrid representation of shallow and deep representation features. For action recognition, the goal-based descriptors will be extended with spatiotemporal texture. For crowd analysis, PREVISION combines swarm-based descriptors with a deep representation. For crisis event detection, PREVISION investigates the implementation of spatio-temporal techniques under a DeepCNN scheme for the detection of crisis events in a near-real time manner. For face recognition, PREVISION leverages facial points detection and a combination of shallow features with a deep convolutional framework.

Regarding steganographic traffic detection, PREVISION processes network traffic traces with and without covert traffic in conjunction with information that such traces contain (or not) secret data.

With respect to information fusion, PREVISION addressed three main challenges using Markov logic networks, the data association problem, the need for a high-quality statistical model, which must be trained using sufficient labelled training data, and the adaptation of the logical (object oriented) model during its usage.

PREVISION also developed a toolkit to identify radicalization tendencies in society at an early stage and, based on this, to develop risk forecasts that allows security authorities in advance to take preventive action. This requires a continuous observation of social processes and especially of violent political milieus.

PREVISION established an open and future-proof platform for providing cutting-edge practical support to LEAs and practitioners in the fight against terrorism, organised crime and cybercrime.

Many work products delivered by the project are available online for consultation. One of these is the deliverable "[Final Set of Training Courses and Material](#)", which may be interesting with respect to the fourth focus area tackled by NOTIONES, namely "*Improvements and Innovations to Various Intelligence Related Training*":

Table 3 Results of the PREVISION project

1	Predictive Policing – Psycho-sociological Models (Initial Release)	REPORT
2	Predictive Policing – Psycho-sociological Models (Refined Release)	REPORT
3	Overall Impact Assessment and Transferability of Results	REPORT
4	Final Set of Training Courses and Material	REPORT
5	End-user Needs and Use Cases (Initial Release)	REPORT
6	Heterogeneous Data Streams Processing Tools (Initial Release)	REPORT
7	Improved Operational and Situational Awareness Applications (Initial Release)	REPORT
8	End-user Needs and Use Cases (Refined Release)	REPORT
9	Heterogeneous Data Streams Processing Tools (Refined Release)	REPORT
10	Improved Operational and Situational Awareness Applications (Refined Release)	REPORT
11	Machine Learning and Automation for Crime Prevention and Investigation (Refined Release)	REPORT

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 project was included in deliverable D5.2 and is ongoing. Many work products delivered by the project are now available online for consultation:

Table 4 Results of the INFINITY project

1	Recommendation report for integrating AI into LEA environments	REPORT
2	Research report on immersive reality, collaborative and analysis methods	REPORT
3	Review of the impacts on cognition, health and well-being for sustained AR/VR headset use	REPORT
4	Mid-term project and societal impact report	REPORT
5	Visualisation report for best practices and techniques	REPORT
6	Survey and Performance Analysis of Deep Learning Based Object Detection in Challenging Environments Author(s): Muhammad Ahmed, Khurram Azeem Hashmi, Alain Pagani, Marcus Liwicki, Didier Stricker, Muhammad Zeshan Afzal Published in: MDPI Sensors, 2021, ISSN 1424-8220 Publisher: Multidisciplinary Digital Publishing Institute (MDPI) DOI: 10.3390/s21155116	PUBLICATION
7	Towards Robust Object Detection in Floor Plan Images: A Data Augmentation Approach Author(s): Shashank Mishra, Khurram Azeem Hashmi, Alain Pagani, Marcus Liwicki, Didier Stricker, Muhammad Zeshan Afzal Published in: MDPI Applied Sciences, 2021, ISSN 2076-3417 Publisher: MDPI DOI: 10.3390/app112311174	PUBLICATION
8	CasTabDetectorRS: Cascade Network for Table Detection in Document Images with Recursive Feature Pyramid and Switchable Atrous Convolution Author(s): Khurram Azeem Hashmi, Alain Pagani, Marcus Liwicki, Didier Stricker, Muhammad Zeshan Afzal Published in: MDPI Journal of Imaging, 2021, ISSN 2313-433X Publisher: MDPI DOI: 10.3390/jimaging7100214	PUBLICATION
9	Current Status and Performance Analysis of Table Recognition in Document Images With Deep Neural Networks Author(s): Khurram Azeem Hashmi; Marcus Liwicki; Didier Stricker; Muhammad Adnan Afzal; Muhammad Ahtsham Afzal; Muhammad Zeshan Afzal	PUBLICATION

	Published in: IEEE Access, 2021, ISSN 2169-3536 Publisher: Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/access.2021.3087865	
10	A Survey of Graphical Page Object Detection with Deep Neural Networks Author(s): Jwalin Bhatt, Khurram Azeem Hashmi, Muhammad Zeshan Afzal, and Didier Stricker Published in: MDPI Applied Sciences, 2021, ISSN 2076-3417 Publisher: MDPI DOI: 10.3390/app11125344	PUBLICATION

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 project was included in deliverable D5.2 and ended in 2021. Many work products delivered by the project are now available online for consultation:

Table 5 Results of CYBER-TRUST project

1	CYBER-TRUST proactive technology tools	Tool
2	CYBER-TRUST network tools	Tool
3	CYBER-TRUST visualisation tool	Tool
4	CYBER-TRUST device tools	Tool
5	CYBER-TRUST information and evidence storage	Tool
6	inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence Author(s): Paris Koloveas, Thanasis Chantzios, Sofia Alevizopoulou, Spiros Skiadopoulos , Christos Tryfonopoulos Published in: Electronics, 10/7, 2021, Page(s) 818, ISSN 2079-9292 Publisher: MDPI DOI: 10.3390/electronics10070818	Publication

7	A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages Author(s): Andrew Ramsdale, Stavros Shiaeles, Nicholas Kolokotronis Published in: Electronics, 9/5, 2020, Page(s) 824, ISSN 2079-9292 Publisher: MDPI DOI: 10.3390/electronics9050824	Publication
8	On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids Author(s): Christos-Minas Mathas, Costas Vassilakis, Nicholas Kolokotronis, Charilaos C. Zarakovitis, Michail-Alexandros Kourtis Published in: Energies, 14/10, 2021, Page(s) 2818, ISSN 1996-1073 Publisher: Multidisciplinary Digital Publishing Institute (MDPI) DOI: 10.3390/en14102818	Publication

EU-HYBNET

Project	EU-HYBNET
Full Title	Empowering a Pan-European Network to Counter Hybrid Threats
GRANT AGREEMENT ID:	883054
Source of information	https://cordis.europa.eu/project/id/883054
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

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academics, industry players, and SME actors across EU collaborating with each other in ever increasing numbers to counter hybrid threats. EU-HYBNET aims to build an empowered, sustainable network beyond the scope of the project through its on-going association with a key partner, The European Centre of Excellence for Countering Hybrid Threats, and it will: define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavours; monitor significant developments in research and innovation; deliver recommendations for uptake and industrialisation of the most promising innovations that address the needs of practitioners, and determine associated priorities for standardisation; establish conditions for enhanced interaction among its members; and persistently strive to increase its membership and continually build network capacity through knowledge exchange incl. exercises. A technology and innovations watch, facilitated by scientific research, will ensure smooth execution of searching, monitoring, identifying and

assessing innovations both under development or already proven, including the level of technology readiness for uptake or industrialisation. EU-HYBNET brings together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats by undertaking an in-depth analysis of gaps and needs and prioritising those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to creation of a roadmap for success and solid recommendations for uptake, industrialisation and standardisation across the European Union.

As such, EU-HYBNET may be a project of interest for NOTIONES with respect not just to the focus area “*Technological needs, solutions, and improvements to the intelligence analysis phase of the Intelligence cycle*”, but also to the focus area “*Improvements and Innovations to Various Intelligence Related Training*”.

Many work products delivered by the project are available online for consultation:

Table 6 Results of EU-HYBNET project

1	Training and Exercise, Scenario delivery	Report
2	Training and exercises delivery on up-to-date topics	Report
3	Established EU-HYBNET Network Platforms	Report
4	Responses to digital disinformation: an evidence-based analysis on the effects of disinformation and the effectiveness of fact-checking/debunking Author(s): Rubén Arcos, Manuel Gértrudix, Cristina Arribas, and Monica Cardarilli Published in: Open Research Europe, 2021 Publisher: European Commission	Publication
5	Quantum as a disruptive technology in Hybrid Threats Author(s): Evaldas Bruze, Monica Cardarilli Published in: JRC Publications Repository, 2021 Publisher: JRC	Publication

LINSEC

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
-----------------	----------------

This MSCA research project on the logic of informal security cooperation (LINSEC) combined the research fields of security studies, IR, international history, and intelligence studies.

LINSEC exploited the access to over 30,000 intelligence records from 1971 to 1979, from a counterterrorism intelligence-sharing framework called the Club de Berne, which is still today's main cooperation platform for informal intelligence-sharing on terrorism. To understand the logic of informal security cooperation, the project analysed four different aspects:

- 1) The prerequisites: what internal and external factors determine whether policymakers seek informal security cooperation;
- 2) Cooperation mechanism: how agencies react to terrorist threats and adapt their habits and modes of security cooperation;
- 3) Formal versus informal: the conditions under which these actors prefer informal over formal security cooperation, and how informal counterterrorism cooperation ties in or comes into conflict with formal alliances;
- 4) Continuity over time: what made informal counterterrorism cooperation effective in the 1970s and what makes it effective today.

Each of these elements form one objective, which then contain a corresponding research, training, and dissemination sub-objective.

The findings of the project contributed to a better-informed public debate about the role of formal and informal cooperation in the fight against terrorism. Considering the practical implications of this research for policymakers and security professionals, LINSEC communication activities targeted practitioners in intelligence, together with policymaking circles and the general public.

LINSEC has significantly advanced the understanding of the international relations of intelligence agencies in three core areas:

- 1) While a common threat was the most determining factor for the creation of security cooperation, a shared mentality fostered increased counterterrorism cooperation.
- 2) Analysed how agencies reacted when a new threat emerged: Libyan supported terrorism in Europe. The results have been published and demonstrated how cooperation served as force multiplier:

[Turning oil into blood: Western intelligence, Libyan covert actions, and Palestinian terrorism \(1973-74\)](#)

Author(s): Aviva Guttman

Published in: Journal of Strategic Studies, 2021, Page(s) 1-28, ISSN 0140-2390

Publisher: Frank Cass Publishers

DOI: 10.1080/01402390.2020.1868995

- 1) Demonstrated how intelligence cooperation can overcome diplomatic crises:

Aviva Guttman. "Covert Diplomacy to Overcome a Crisis: German and Israeli Intelligence after the Munich Olympics Attack," forthcoming in the Journal of Cold War Studies.

The project ended in August 2022.

ROXANNE

Project	ROXANNE
Full Title	Real time network, text, and speaker analytics for combating organized crime
GRANT AGREEMENT ID:	833635
Source of information	https://cordis.europa.eu/project/id/833635
EU contribution	€ 6 999 458,75
Coordinator	FONDATION DE L'INSTITUT DE RECHERCHE IDIAP
Website:	https://www.idiap.ch/fr
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999644074/833635
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2019
End Date	31 December 2022
Description of any problem encountered	



Fighting organised crime has become a top priority for European law enforcement agencies (LEA). The EU-funded ROXANNE project intends to combine new speech technologies, face recognition and network analysis to facilitate the identification of criminals. Specifically, ROXANNE will develop a platform that will increase agencies' capabilities via voice recognition, language and video technologies. The project will support LEA's activities through multilanguage applications based on voice, text and face technologies. ROXANNE, in conformity with Interpol and EU regulations, will be tested on real case data in nine EU Member States.

The technical development will be centred around the ROXANNE platform, which will enhance criminal network analysis capabilities by providing a framework for extracting evidence and actionable intelligence based on speech, language and video technologies. The intention is not to replace humans but automate time-consuming tasks, and support LEA decision-making. Its early version will offer preliminary SLT, VA and NA capabilities to collect end-user feedback. The final version will provide multilingual, probabilistic tools interfacing SLT and NA technologies, boosted by natural language processing (NLP) and relation analysis in the synoptic criminal activity graph. ROXANNE will achieve full compliance with relevant INTERPOL and EU legal and ethical frameworks, including innovative approaches to data protection management such as privacy by design.

Special efforts will be expended to ensure ROXANNE outcomes achieve widespread adoption by law enforcement. The effort will be enhanced through a series of education and awareness campaigns and the direct involvement of LEAs from nine European countries, that will test our solutions on real case data.

The project is ongoing and many work products delivered by the project are available online for consultation:

Table 7 Results of ROXANNE project

1	OdiEnCorp 2.0 Author(s): Parida, Shantipriya; Bojar, Ondřej Published in: Charles University, Faculty of Mathematics and Physics, Institute of Formal and Applied Linguistics (UFAL)	Dataset via OpenAIRE 
2	Hindi Visual Genome 1.1 Author(s): Parida, Shantipriya; Bojar, Ondřej Published in: Charles University, Faculty of Mathematics and Physics, Institute of Formal and Applied Linguistics (UFAL)	Dataset via OpenAIRE 
3	Technical specifications and detailed architecture	Report
4	Inferring Highly-dense Representations for Clustering Broadcast Media Content Author(s): Esaú Villatoro-Tello, Shantipriya Parida, Petr Motliceck, Ondřej Bojar Published in: Prague Bulletin of Mathematical Linguistics, 115/1, 2020, Page(s) 31-50, ISSN 1804-0462 Publisher: Creative Commons CC BY-NC-ND DOI: 10.14712/00326585.004	Publication
5	Description of the integration toolkit, guidelines, plan	Report

NESTOR

Project	NESTOR
Full Title	aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders
GRANT AGREEMENT ID:	101021851
Source of information	https://cordis.europa.eu/project/id/101021851
EU contribution	€ 4 999 578,13 of a total costs : € 6 108 593,75
Coordinator	HELLENIC POLICE
Website:	http://www.astynomia.gr/index.php?lang=EN
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/911255928/101021851
Funding Scheme	IA – Innovation Action
Start Date	1 November 2021
End Date	30 April 2023

The European Community faces a number of challenges both at a political and at a tactical level. Irregular migration flows exerting significant pressure to the relevant authorities and agencies that operate at border

territories. Armed conflicts, climate pressure and unpredictable factors occurring at the EU external borders, have increased the number of the reported transnational crimes. Smuggling activity is a major concern for Eastern EU Borders particularly, as monitoring the routes used by smugglers is being hindered by mountainous, densely forested areas and rough lands aside with sea or river areas. Due to the severity and the abrupt emergence of events, the relevant authorities operate for a long-time interval, under harsh conditions, 24 hours a day. NESTOR aims to demonstrate a fully functional next generation holistic border surveillance system providing pre-frontier situational awareness beyond maritime and land border areas following the concept of the European Integrated Border Management. NESTOR long-range and wide area surveillance capabilities for detection, recognition classification and tracking of moving targets (e.g. persons, vessels, vehicles, drones etc.) is based on optical, thermal imaging and Radio Frequency (RF) spectrum analysis technologies fed by an interoperable sensors network including stationary installations and mobile manned or unmanned vehicles (aerial, ground, water, underwater) capable of functioning both as standalone, tethered and in swarms. NESTOR BC3i system will fuse in real-time border surveillance data combined with web and social media information, creating and sharing a pre-frontier intelligent picture to local, regional and national command centres in AR environment being interoperable with CISE and EUROSUR.

The project is ongoing. No work products delivered by the project are available online for consultation, yet.

CREST

Project	CREST
Full Title	Fighting Crime and TerrorRism with an IoT-enabled Autonomous Platform based on an Ecosystem of Advanced IntelligEnce, Operations, and InveStigation Technologies
GRANT AGREEMENT ID:	833464
Source of information	https://cordis.europa.eu/project/id/833464
EU contribution	€ 6 999 078,75 of a total costs : € 6 999 078,75
Coordinator	SERVICIUL DE PROTECTIE SI PAZA
Website:	https://www.spp.ro/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/937433609/833464
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2019
End Date	28 February 2023
Description of any problem encountered	

CREST aims to equip LEAs with an advanced prediction, prevention, operation, and investigation platform by leveraging the IoT ecosystem, autonomous systems, and targeted technologies and building upon the concept of multidimensional integration and correlation of heterogeneous multimodal data streams (ranging from online content to IoT-enabled sensors) for a) threat detection and assessment, b) dynamic mission planning and adaptive navigation for improved surveillance based on autonomous systems, c) distributed command and control of law enforcement missions, d) sharing of information and exchange of digital evidence based on blockchain, and e) delivery of pertinent information to different stakeholders in an

interactive manner tailored to their needs. CREST will also provide chain-of-custody, and path-to-court for digital evidence. Human factors and societal aspects will also be comprehensively addressed, while information packages for educating the wider public on identifying threats and protecting themselves will be prepared and distributed. The platform development will adopt ethics and privacy by-design principles and will be customisable to the legislation of each member state. CREST will be validated in field tests and demonstrations in three operational uses cases: 1) protection of public figures in motorcades and public spaces, 2) counter terrorism security in crowded areas, and 3) Cross-border fight against organised crime (e.g. firearms trafficking). Extensive training of LEAs' personnel, hands-on experience, joint exercises, and training material, will boost the uptake of CREST tools and technologies. The final result of CREST is expected to be an innovative prediction, prevention, operation, and investigation platform and solutions which aim to improve the state-of-the-art in several scientific and technological fields, thus facilitating the implementation of the promised impact; these include:

- i. Information extraction and representation from multimodal stream data for enabling the accurate and timely interpretation of sensor readings based IoT fusion and perform visual analysis on multimodal data streams.
- ii. Artificial Intelligence for dynamic mission planning and adaptive navigation in autonomous systems for the better surveillance of public areas by conducting dynamic UxV swarm optimisation and optimised rerouting in case of abnormal situations encountered during the execution of LEA operations.
- iii. Multimodal information analysis and correlation for threat detection for assessing threats and providing early warnings based on multimodal data analytics.
- iv. Distributed command and control of law enforcement missions and information sharing for facilitating the efficient collaboration of LEAs across organisational boundaries.
- v. Multimodal information delivery for improving situational awareness, through the provision of pertinent information based on visual analytics, augmented reality, and mobile applications for dynamic on-site information.

As such, EU-HYBNET may be a project of interest for NOTIONES with respect not just to the focus area “Technological needs, solutions, and improvements to the intelligence analysis phase of the Intelligence cycle”, but also to the focus area “Improvements and Innovations to Various Intelligence Related Training”.

The project is ongoing. Two publications produced by the project are available online for consultation:

Table 8 Results of CREST project

1	<p>Autonomous and Cooperative Design of the Monitor Positions for a Team of UAVs to Maximize the Quantity and Quality of Detected Objects</p> <p>Author(s): Dimitrios I. Koutras, Athanasios Ch. Kapoutsis, Elias B. Kosmatopoulos</p> <p>Published in: IEEE Robotics and Automation Letters, 5/3, 2020, Page(s) 4986-4993, ISSN 2377-3766</p> <p>Publisher: IEEE ROBOTICS AND AUTOMATION LETTERS</p> <p>DOI: 10.1109/Ira.2020.3004780</p>	Publication
2	<p>Spatio-temporal activity detection and recognition in untrimmed surveillance videos</p>	Publication

<p>Author(s): Konstantinos Gkountakos, Despoina Touska, Konstantinos Ioannidis, Theodora Tsirikika, Stefanos Vrochidis, Ioannis Kompatsiaris.</p> <p>Published in: 2021 International Conference on Multimedia Retrieval, August 21-24, 2021, 2021</p> <p>Publisher: ACM International Conference on Multimedia Retrieval, ICMR 2021</p> <p>DOI: 10.5281/zenodo.4748350</p>	
---	--

CTCMR

Project	CTCMR
Full Title	Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies
GRANT AGREEMENT ID:	670172
Source of information	https://cordis.europa.eu/project/id/670172
EU contribution	€ 2 479 810 of a total costs : € 2 479 810
Coordinator	TECHNISCHE UNIVERSITEIT DELFT
Website:	http://www.tudelft.nl/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999977366/670172
Funding Scheme	EXCELLENT SCIENCE - European Research Council (ERC)
Start Date	1 January 2016
End Date	30 September 2021
Description of any problem encountered	

Terrorism continues to present a major threat to global security, and tackling it effectively requires ethically complex decision-making. GTCMR's research sought to help decision makers navigate the grey areas. Counterterrorism is by necessity a collective responsibility, involving the police, military and intelligence agencies, alongside non-security actors. It is riddled with difficult ethical questions, such as how to save lives without infringing human rights. Efforts routinely raise questions about not only which strategies and tactics are effective, but also which are consistent with the values of liberal democracies and permissible within their legal frameworks.

The GTCMR project, supported by the European Research Council, has helped develop the relatively nascent field of counterterrorism ethics, by introducing ethical analyses. GTCMR was the first to apply the designing-in-ethics methodology to counterterrorism issues. Usually applied to new technology, the methodology asks developers to consider the consequences of their decisions related to issues of design, application and access. As these questions become routine and embedded in daily practice, so working cultures change over time.

Ethical analysis of the issues involved, underpinned by empirical information, enables guidelines to be formulated that give ethical direction to policymakers and practitioners. The range of ethically controversial antiterrorism tactics GTCMR reviewed included: targeted killing; preventive detention; censorship of disinformation and online content; response to weapons of mass destruction and terrorist attacks; DNA

collection and storage; biometric identification, such as facial recognition; and the application of artificial intelligence. GTCMR based their research on both the empirical studies of other scholars, augmented by their own research. This consisted chiefly of in-depth interviews with a variety of stakeholders, including those able to influence policy and practice, such as past and present heads of security agencies, including former directors of the CIA.

The project ended in 2021. Many publications produced by the project are available online for consultation:

Table 9 Results of CTCMR project

1	Drone Strikes Author(s): Seumas Miller, Bruce Arrigo, Geoffrey Golson Published in: The SAGE Encyclopedia of Surveillance, Security, and Privacy, 2018 Publisher: SAGE Publications, Inc. DOI: 10.4135/9781483359922.n142	Publication
2	Cyber-war Author(s): Seumas Miller, Bruce Arrigo, Geoffrey Golson Published in: The SAGE Encyclopedia of Surveillance, Security, and Privacy, 2018 Publisher: SAGE Publications, Inc. DOI: 10.4135/9781483359922.n119	Publication
3	National Security Agency Leaks Author(s): Seumas Miller, Bruce Arrigo, Geoffrey Golson Published in: The SAGE Encyclopedia of Surveillance, Security, and Privacy, 2018 Publisher: SAGE Publications, Inc. DOI: 10.4135/9781483359922.n297	Publication
4	Terrorism Author(s): Seumas Miller, Bruce Arrigo, Geoffrey Golson Published in: The SAGE Encyclopedia of Surveillance, Security, and Privacy, 2018 Publisher: SAGE Publications, Inc. DOI: 10.4135/9781483359922.n448	Publication
5	Torture Author(s): Seumas Miller Published in: Oxford Bibliographies in Philosophy, 2017 Publisher: Oxford University Press DOI: 10.1093/obo/9780195396577-0353	Publication

3.3 Secure Data Sharing

A search was launched in the second run of task T5.2 on the research projects relevant for the NOTIONES focus area “*Technological Solutions to Secure Data Sharing and Dissemination (internally and externally)*”. Two interesting projects were found. The table below enlists these projects:

acronym	title	start-end year	Mapped at
INSPECTr	Intelligence Network and Secure Platform for Evidence Correlation and Transfer	2019-2023	2 nd search round
I-LEAD	Innovation - Law Enforcement Agencies Dialogue	2017-2023	2 nd search round

Table 10 Selected projects for Secure Data Sharing

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

INSPECTr

Project	INSPECTr
Full Title	Intelligence Network and Secure Platform for Evidence Correlation and Transfer
GRANT AGREEMENT ID:	833276
Source of information	https://cordis.europa.eu/project/id/833276/it
EU contribution	€ 6 997 910 of a total costs : € 6 997 910
Coordinator	UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN
Website:	http://www.ucd.ie/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999974359/833276
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2019
End Date	28 February 2023

Intelligence Network & Secure Platform for Evidence Correlation and Transfer (INSPECTr). The principal objective of INSPECTr is to develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level. This data will originate from the outputs of free and commercial digital forensic tools complemented by online resource gathering. Using both structured and unstructured data as input, the developed platform will facilitate the ingestion and homogenisation of this data with increased levels of automatised, allowing for interoperability between outputs from multiple data formats.

Various knowledge discovery techniques allow the investigator to visualise and bookmark important evidential material and export it to an investigative report. In addition to providing basic and advanced (cognitive) cross-correlation analysis with existing case data, this technique will aim to improve knowledge discovery across exhibit analysis within a case, between separate cases and ultimately, between

interjurisdictional investigations. INSPECTr will deploy big data analytics, cognitive machine learning and blockchain approaches to significantly improve digital and forensics capabilities for Pan-European LEAs.

INSPECTr intends to reduce the complexity and the costs in law enforcement agencies and related actors to use leading edge analytical tools proportionally and in line with relevant legislation (including fundamental rights), with extended options for multi-level and cross-border collaboration for both reactive and preventive policing and facilitate the detection/prediction of cybercrime operations/trends. The final developed platform will be freely available to all LEAs.

The project is ongoing. Many work products delivered by the project are available online for consultation:

Table 11 Results of INSPECTr project

1	Initial Legislative compliance relating to law-enforcement powers and evidence requirements	Report
2	Reference Digital Forensics Domain Model	Report
3	e-Codex infrastructure evaluation in the context of deployment in LLs	Report

I-LEAD

Project	I-LEAD
Full Title	Innovation - Law Enforcement Agencies Dialogue
GRANT AGREEMENT ID:	740685
Source of information	https://cordis.europa.eu/project/id/740685
EU contribution	€ 3 483 717,50 of a total costs : € 3 483 717,50
Coordinator	THE NATIONAL POLICE OF THE NETHERLANDS
Website:	http://www.politie.nl/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/942970272/740685
Funding Scheme	CSA – Coordination and Support Action
Start Date	1 September 2017
End Date	28 February 2023

I-LEAD's focus is on the incapability of groups of operational Law Enforcement Agencies (LEA) practitioners defining their needs for innovation. This will be done in a methodological way, also with the help of the research & industrial partners supplemented by a broad range of committed stakeholders. I-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-European LEA network. Earlier funded European research with a high technology readiness level as well as pipeline technologies will be closely monitored and assessed on its usefulness. Where possible a direct uptake from this research will be facilitated and implemented in the ENLETS and ENFSI networks supporting the action. I-LEAD will indicate priorities in five practitioner groups as well as aspects that needs (more)

standardization and formulate recommendations how to incorporate these in procedures. As a final step, I-LEAD will advise the Member States through the existing EDBP-ESTP procurement group about how the outcomes of this project could be used in Pre-Commercial Procurement and Public Procurement of Innovation activities.

The project is ongoing. One work product delivered by the project is available online for consultation so far:

Table 12 Results of I-LEAD project

1	Report on the EU standardisation and procurement in area of security	Report
---	--	--------

Many other work products are available on the project website⁵, such as reports on digital investigations, crime scene recording and documentation, vehicle mitigation, crime as a service, and recommendations on standardisation and procurement.

3.4 Cybersecurity and Cybercrime

A search was launched in the second run of task T5.2 on the research projects relevant for cyber-security and cyber-criminality. Six interesting projects were found, two already included in the first run of the task, and four newly found. The table below enlists these projects:

Table 13 Selected projects for Cybersecurity and Cybercrime

acronym	title	start-end year	Mapped at
CONCORDIA	Cyber security cOMpeteNCe fOR Research and InnovAtion	2019-2022	1 st search round
ECHO	European network of Cybersecurity centres and competence HUB for Innovation and Operations	2019-2023	1 st search round
REACT	REactively Defending against Advanced Cybersecurity Threats	2018-2021	2 nd search round
CyberSANE	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures	2019-2022	2 nd search round
CC-DRIVER	Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour A Research	2020-2023	2 nd search round
CyberSec4Europe	Cyber Security Network of Competence Centres for Europe Critical Infrastructures	2019-2022	2 nd search round

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

⁵ <http://i-lead.eu/publications/>

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.

The project was included in deliverable D5.2 and it is ongoing. Many work products delivered by the project are available online for consultation:

Table 14 Results of CONCORDIA project

Software via OpenAIRE (3)	
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"	Author(s): Papadamou, Kostantinos; Zannettou, Savvas; Blackburn, Jeremy; De Cristofaro, Emiliano; Stringhini, Gianluca; Sirivianos, Michael

https://doi.org/10.5281/zenodo.4580891	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
Datasets via OpenAIRE	
Discovery and classification of Twitter bots	Author(s): Alexander Shevtsov; Maria Oikonomidou; Despoina Antonakaki; Polyvios Pratikakis; Alexandros Kanterakis; Sotiris Ioannidis; Paraskevi Fragopoulou Published in: Zenodo
Responses to AHP-style questionnaires regarding the publication "D-Score: A Novel Expert-Based Method for Assessing the Detectability of IoT-Related Cyber-Attacks"	Author(s): Meidan, Yair; Benatar, Daniel; Biton, Ron; Shabtai, Asaf Published in: Zenodo
CADESH Dataset: Collaborative Anomaly Detection for Smart Homes	Author(s): Meidan, Yair; Avraham, Dan; Libhaber, Hanan; Shabtai, Asaf Published in: Zenodo
Dataset of transactions of 10 Ethereum addresses controlled by a private key, each has at least 2000 output transactions, which include a transfer of cryptocurrency, and all transactions are performed within no longer than three months period	Author(s): Blaž Podgorelec Published in: Zenodo
Dataset Using TLS Fingerprints for OS Identification in Encrypted Traffic	Author(s): Martin, Laštovička; Stanislav, Špaček; Petr, Velan; Pavel, Čeleda Published in: Zenodo

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 was included in deliverable D5.2. 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.

As such, ECHO may be a project of interest for NOTIONES with respect not just to cybersecurity and cybercriminality, but also to the focus area *“Improvements and Innovations to Various Intelligence Related Training”*.

REACT

Project	REACT
Full Title	REactively Defending against Advanced Cybersecurity Threats
GRANT AGREEMENT ID:	786669
Source of information	https://cordis.europa.eu/project/id/786669
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

Security is a vital property for every operational system and network. As systems become more powerful and, in many aspects, more complex, advanced cyber-attacks impose new threats for important operations of our society. Computer systems assist core functions of hospitals, energy centers, logistics, and communications, to name a few, and compromising such systems may have severe consequences for everyone of us. Despite the evolution of computer systems, current security defenses-although they have been substantially improved in the last decade-seem not really enough to stop advanced cyber attacks. Systems still suffer from vulnerabilities, despite the many active or passive defenses in place that have been developed in the last decades. The REACT project advocates that we should change the rules of the cyber attackers' game and challenge the asymmetry. Instead of following the cyber attackers, researchers should try to forecast where attackers will strike next and to use this information (i) to fortify potential targets to withstand the attack and (ii) to wire targets up with forensic hooks and make them "forensics ready". To make all this possible at a reasonable performance cost, REACT proposes selective fortification, a mechanism that combines traditional passive and active defense approaches into a new reactive mode of operation.

The project ended in 2021. Many work products delivered by the project are available online for consultation:

1	Selective Isolation and Protection	Report
2	Vulnerability Discovery	Database
3	Report on the Validation Experiments	Report
4	Report on Forensic-Readiness Techniques	Report
5	Selective Software Hardening	Report

CyberSANE

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

In today's digital era, the increased usage of information technology in modern CIIs makes them vulnerable to cyber-related crime. The EU-funded CyberSANE project will enhance their security and resilience by providing a dynamic collaborative warning and response system. This will support and guide security officers to recognise, identify, dynamically analyse, forecast, treat and respond to advanced persistent threats and

handle their daily cyber incidents utilising and combining both structured data and unstructured data coming from social networks and the dark web. CyberSANE aims to design and implement an advanced, configurable and adaptable, Security and Privacy Incident Handling Systems, towards security incident detection and handling, composed of five independent but collaborative components: LiveNet (Live Security Monitoring and Analysis), DarkNet (Deep and Dark Web Mining and Intelligence), HybridNet (Data Fusion, Risk Evaluation and Event Management), ShareNet (Intelligence and Information Sharing and Dissemination), and PrivacyNet (Privacy & Data Protection Orchestrator). These five components work together to improve, intensify and coordinate the overall security efforts for the effective and efficient identification, investigation, mitigation and reporting of realistic multi-dimensional attacks within the interconnected web of cyber assets in the CII and security events. Through extensive validation, CyberSANE will act as a catalyst for improving the innovation in cybersecurity capacity by increasing the privacy and the security of online healthcare, energy, and maritime transportation services.

The project ended in August 2022. Many work products delivered by the project are available online for consultation:

1	Intelligence and Information Sharing models Specifications	Report
2	Cyber Incident handling Trend Analysis	Report
3	Prevention and response to advanced threats and anomalies	Report
4	Towards an Interpretable Deep Learning Model for Mobile Malware Detection and Family Identification Author(s): Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone Published in: Computers & Security, 2021, Page(s) 102198, ISSN 0167-4048 Publisher: Pergamon Press Ltd. DOI: 10.1016/j.cose.2021.102198	Publication
5	Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures Author(s): Spyridon Papastergiou, Haralambos Mouratidis, Eleni-Maria Kalogeraki Published in: Evolving Systems, 2020, ISSN 1868-6478 Publisher: Springer Verlag DOI: 10.1007/s12530-020-09335-4	Publication

CC-DRIVER

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

CC-DRIVER uses a multidisciplinary approach from the domains of psychology, criminology, anthropology, neurobiology and cyberpsychology to investigate and explain drivers of new forms of criminality. Scientific investigation of drivers into cybercrime, the impact of online disinhibition and the effect of youth decision-making processes have informed the project's evidence-based intervention and deterrence strategies. CC-DRIVER's measures are designed to educate regarding criminality and to divert youth from crime.

By investigating 'cybercrime-as-a-service', the project will design policy templates for combatting online cybercrime and produce a youth self-assessment online metric tool designed to help understand cybercriminal behaviour and prompt positive pathways. The project partners are developing a self-assessment questionnaire to enable SMEs, CSOs and other stakeholders to assess their vulnerability to cybercrime attacks. CC-DRIVER is delivering opportunities for EU LEAs (Law Enforcement Agencies) to exchange knowledge and experiences with a view to fostering common European approaches and strengthening the European Security Union. The project will produce tools for LEAs to gather evidence and investigate and mitigate cybercrime operations. Finally, the project is also conducting a comparative analysis of cybercrime legislation and policy in eight Member States.

The project has established a number of advisory boards and working groups in its first 18 months. It created a 24-member Stakeholder Board in the early stages. The Stakeholder Board members represent a wide range of stakeholder groups, including LEAs. The project's separate LEA Working Group meet regularly to exchange knowledge and experiences. It has also established a cluster of ten EU-funded security projects involving LEA partners to share knowledge. An ethics advisory board has also been established, comprising five external experts to have their independent views on solutions proposed by the partners.

Results

Based on an initial literature review, the consortium has explored the phenomenon of cybercrime in four dimensions, as well as the challenges arising from them: (1) working definitions and typologies of cybercrime, (2) general legal framework, (3) current evolution of cybercrime, investigating the concept of cybercrime-as-a-service, (4) characteristics of the profiles of the offenders and victims for a selection of cybercrimes, as well as the *modi operandi* of the perpetrators.

The partners then conducted a review of the techniques, tools and tactics of cyber criminals and cybercrime-as-a-service and investigated the technological developments that facilitate criminality, the availability of hacking tools online, cryptocurrencies and the widespread use of anonymity and the Dark Web. They focused on human drivers that enable and/or allow humans to act differently online. The consortium's resulting landscape study on "cybercrime-as-a-service" (CaaS) is available on the project website.

The partners are currently finalising a report on the drivers of cyber juvenile delinquency. It reviews motivations and characteristics of offenders and factors associated with eight different types of cybercriminal acts (including illegal access, digital piracy, identity theft, cyberbullying, non-consensual sharing of intimate images, online hate speech, illegal virtual marketplaces and organised crime) across the spectrum of cybercriminality. In the first 18 months partners reviewed the literature in the key disciplines of criminology, psychology, cyberpsychology, neuroscience and digital anthropology. Partners conducted 36 semi-structured

interviews with experts. To gather empirical evidence, the partners conducted a survey of 16- to 19-year-olds, 1000 in each of nine European countries, on the drivers of juvenile cybercrime. The survey measured 38 variables. The sampled countries included France, Spain, Germany, Italy, Netherlands, Romania, Sweden, Norway and the UK.

The project has also produced an online youth self-assessment metric tool designed to help understand cybercriminal behaviour and to prompt positive pathways. Furthermore, the project has developed an online, self-assessment questionnaire that SMEs, CSOs and other stakeholders can use to assess, anonymously, their vulnerability to cybercrime attacks. The user will receive a score and suggestions for addressing vulnerabilities. And for LEAs, CC-DRIVER is producing tools to gather evidence using cloud forensics and investigate and mitigate cybercrime operations. Partners have conducted a review of cybersecurity policies in eight countries (France, Germany, Italy, Netherlands, Romania, Spain, Sweden and the United Kingdom). This task involved desktop research as well as special interest group roundtables with subject matter experts to perform a review of five elements (strategy, legislation, engagement, enforcement and assessment) in the cybercrime landscape. The partners conducted a gap analysis of cybersecurity legislation and cybercriminality policies in the eight countries. They identified where legislation and policies are the same, similar or different with a view to recommending changes. The analysis was supported by questionnaires and workshops completed and attended by the task consortium.

CyberSec4Europe

Project	CyberSec4Europe
Full Title	Cyber Security Network of Competence Centres for Europe Critical Infrastructures
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 December 2022

As pilot for a Cybersecurity Competence Network, CyberSec4Europe project will test and demonstrate potential governance structures for the network of competence centres using the best practices examples from the expertise and experience of the participants, including concepts like CERN. CyberSec4Europe will support addressing key EU Directives and Regulations, such as GDPR, PSD2, eIDAS, and ePrivacy, and help to implement the EU Cybersecurity Act including, but not limited to supporting the development of the European skills-base, the certification framework and ENISA's role. The 26 ECSO participants in CyberSec4Europe are active in all 6 ECSO Working Groups, including chairing many subgroups in cybersecurity certification, vertical sectors, and international cooperation, as well as having representatives on the ECSO Board of Directors and the Cybersecurity Public-Private Partnership Board. CyberSec4Europe

participants address 14 key cybersecurity domain areas, 11 technology/applications elements and nine crucial vertical sectors. The project demonstration cases will address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation. In addition to the demonstration of the governance structure and the operation of the network, CyberSec4Europe will develop a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project.

The project is ongoing. Many work products delivered by the project are available online for consultation:

1	Framework and Toolset for conformity	Toolset
2	Cross sectoral cybersecurity building blocks	Report
3	Usable security & privacy methods and rec-ommendations	Report
4	Research and Development Roadmap 2	Roadmap
5	Report on existing cyber ranges, requirements	Report
6	Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence Author(s): Davy Preuveneers, Wouter Joosen Published in: Journal of Cybersecurity and Privacy, 1/1, 2021, Page(s) 140-163, ISSN 2624-800X Publisher: MDPI DOI: 10.3390/jcp1010008	Publication

3.5 Artificial Intelligence (AI)

Taking into account the number of projects found with regards to Artificial Intelligence related topics relevant to NOTIONES, an ad hoc additional category has been created. Seven projects were found, which are of particular interest with regards to their focus over AI aspects. The table below enlists these projects:

Table 15 Selected projects for Artificial Intelligence

acronym	title	start-end year
pop AI	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights	2021-2023
ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement	2021-2024
STARLIGHT	Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats	2021-2025
APPRAISE	fAcilitating Public & Private secuRity operAtors to mitigate terrorism Scenarios against soft targEts	2021-2023
IRIS	artificial Intelligence threat Reporting and Incident response System	2021-2024
TAILOR	Foundations of Trustworthy AI - Integrating Reasoning, Learning and Optimization	2020-2023
AIDA	Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies	2020-2023

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

pop AI

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	https://cordis.europa.eu/project/id/101022001
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

Use of artificial intelligence (AI) is increasing in a wide range of applications, making it the focus of law enforcement agencies (LEA) concerned with safeguarding privacy and fundamental rights. The EU-funded pop AI project will work to boost trust in AI by increasing awareness and current social engagement, consolidating distinct spheres of knowledge by academics and non-academics, and delivering a unified European view and recommendations. The project will create an ecosystem and the structural basis for a sustainable and inclusive European AI hub for LEA. It will use existing knowledge and extensive studies to identify and document the direct and indirect stakeholders from the security and AI sectors as well as their corresponding views while ensuring equitable gender and diversity representation.

The core vision of pop AI is to foster trust in AI for the security domain via increased awareness, ongoing social engagement, consolidating distinct spheres of knowledge (including theoretical & empirical knowledge by academics & non-academics) and offering a unified European view across LEAs, and specialised knowledge outputs (recommendations, roadmaps, etc.), while creating an ecosystem that will form the structural basis for a sustainable and inclusive European AI hub for Law Enforcement. Pop AI approaches the call requirements under a sustainable ecosystem perspective, aiming to create cross disciplinary ecosystem AI-LEA ethics hubs. First, we aim to utilize existing knowledge, but also an extensive set of studies, to identify and record the direct and indirect stakeholders of the "security and AI" setting, as well as their respective points of view (concerns, perceived opportunities, challenges). This recording aims to further delve into the dynamic interactions of these stakeholders and ensure appropriate gender and diversity representation in the participatory processes. This way Pop AI will tap into the rich knowledge of security practitioners, civil society organisations, and citizens, as well as Social Sciences and Humanities experts, to define appropriate interactions and material (e.g. talks, cross-disciplinary reports, workshops, online resources) that will allow co-creation within the ecosystem. Such interaction will empower a Positive Sum viewpoint when participating in innovation processes related to security and AI (from idea inception, to product development and application).

ALIGNER

Project	ALIGNER
Full Title	Artificial Intelligence Roadmap for Policing and Law Enforcement
GRANT AGREEMENT ID:	101020574
Source of information	https://cordis.europa.eu/project/id/101020574
EU contribution	€ 1 499 960 of a total costs : € 1 499 960
Coordinator	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV
Website:	http://www.fraunhofer.de/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999984059/101020574
Funding Scheme	CSA – Coordination and Support action
Start Date	1 October 2021
End Date	30 September 2024
Description of any problem encountered	N/A

The EU-funded ALIGNER project aims to unite European actors who have concerns about AI, law enforcement and policing to jointly identify and discuss how to enhance Europe's security whereby AI strengthens law enforcement agencies while providing benefits to the public. The project's work will help pave the way for an AI research roadmap.

ALIGNER aims to bring together European actors concerned with Artificial Intelligence, Law Enforcement, and Policing to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports LEAs while simultaneously empowering, benefiting, and protecting the public.

To achieve this, ALIGNER will (1) Facilitate communication and cooperation between actors from law enforcement, policing, policy-making, research, industry, and civil society about the changing dynamics of crime patterns relevant to the use of AI by establishing a workshop series; (2) Identify the capability enhancement needs of European LEAs; (3) Identify, assess, and validate AI technologies with potential for LEA capability enhancement by implementing a technology watch process that includes impact and risk assessments; (4) Identify ethical, societal, and legal implications of the use of AI in law enforcement; (5) Identify means and methods for preventing the criminal use of AI via the development of a taxonomy of AI-supported crime; (6) Identify policy and research needs related to the use of AI in law enforcement by mapping practitioner needs and emerging crime patterns with identified AI technologies; and (7) Employ the gathered insights in order to incrementally develop and maintain an AI research roadmap. ALIGNER ensures that project results are applicable and relevant by not only including three LEA organisations as full partners of the project, but also establishing two external advisory boards, one for LEA practitioners and one for researchers, industry professionals, ethicists, and civil society.

STARLIGHT

Project	STARLIGHT
Full Title	Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats
GRANT AGREEMENT ID:	101021797
Source of information	https://cordis.europa.eu/project/id/101021797
EU contribution	€ 17 000 000 of a total costs : € 8 835 263,75
Coordinator	COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Website:	http://www.cea.fr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999992401/101021797
Funding Scheme	IA - Innovation action
Start Date	1 October 2021
End Date	30 September 2025

The EU-funded STARLIGHT project will increase awareness, ability, adoption, and long-term results of AI applications in European LEAs. It will improve the widespread understanding of AI across LEAs to reinforce their investigative and cybersecurity operations and support legal, ethical, and societal values. By offering opportunities to exploit AI tools and solutions, STARLIGHT will ensure LEAs can protect their own AI systems, and increase LEA expertise and capacity against AI-supported crime and terrorism. The project will raise high-quality datasets, an interoperable and standardised framework, and an AI hub to enhance the EU's strategic autonomy in AI.

STARLIGHT presents an inclusive and sustainable vision for increasing the awareness, capability, adoption and long-term impact of AI in Europe for LEAs. Five strategic goals underpin STARLIGHT's approach: (1) Improve the widespread UNDERSTANDING of AI across LEAs to reinforce their investigative and cybersecurity operations and the need to uphold legal, ethical and societal values; (2) Provide opportunities to LEAs to EXPLOIT AI tools and solutions in their operational work that are trustworthy, transparent and human-centric; (3) Ensure that LEAs can PROTECT their own AI systems through privacy- and security-by-design approaches, better cybersecurity tools and knowledge; (4) Raise LEAs' expertise and capacity to COMBAT the misuse of AI-supported crime and terrorism; and (5) BOOST AI for LEAs in Europe through high-quality datasets, an interoperable and standardised framework for long term sustainability of solutions, and the creation of an AI hub for LEAs that supports a strong AI security industry and enhances the EU's strategic autonomy in AI. STARLIGHT will ensure European LEAs lead the way in AI innovation, autonomy and resilience, addressing the challenges of now and the future, prioritising the safety and security of Europe for all.

APPRAISE

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

The EU-funded APPRAISE project will develop an integrated threat intelligence solution designed for protecting the augmented cities environment. It will perform a continuous and effective monitoring of online sources and physical sensors to identify potential threats and improve strategies for protection of soft targets (such as shopping malls and stadiums), while preserving the freedom of citizens. Building on the latest advances in big data analysis, AI and advanced visualisation, the project will offer unprecedented capabilities to predict and identify criminal and terrorist acts and enhance the private-public collaboration of security actors.

APPRAISE aims to build on the latest advances in big data analysis, artificial intelligence, and advanced visualisation to create an integral security framework that will improve both the cyber/physical security and safety of public spaces by enabling a proactive, integrated, risk-based, and resilience-oriented approach. This framework will be designed to support the secured private-public collaboration and optimise the coordination of operations involving private security staff, private operators, and law enforcement agencies. APPRAISE will offer unprecedented capabilities to predict and identify criminal and terrorist acts and enhance the operational collaboration of security actors before, during, and after an incident occurs. Social, Ethical, Legal, and Privacy observatories bringing together LEAs, private operators, technology experts, psychologists, sociologists, and society representatives will ensure full conformity of the developed tools with current EU legislation and citizens' acceptance, preparing the ground for successful exploitation. APPRAISE will demonstrate its solutions in four complementary pilot sites: a tennis tournament in Italy, a transnational cycling tour with stages in France and Spain, an international fair in Poland, and a mall in Slovenia.

IRIS

Project	IRIS
Full Title	artificial Intelligence threat Reporting and Incident response System
GRANT AGREEMENT ID:	101021727
Source of information	https://cordis.europa.eu/project/id/101021727
EU contribution	€ 4 918 790 of a total costs : € 5 678 075
Coordinator	INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES INOVACAO

Website:	http://www.inov.pt/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999620503/101021727
Funding Scheme	IA - Innovation action
Start Date	1 September 2021
End Date	31 August 2024

The EU-funded IRIS project will address the challenges of IoT- and AI-driven ICT systems through a collaborative-first approach centred around computer security incident response teams (CERTs/CSIRTs). Specifically, the project equips CERTs/CSIRTs with a state-of-the-art incident response toolkit for assessing, detecting, responding to and sharing information regarding threats and vulnerabilities of IoT and AI-driven ICT systems. The project will establish the first dedicated online training and cyber exercises to prepare CERTs/CSIRTs to collaboratively protect critical infrastructures and systems against cross-border AI and IoT threats. Pilot demonstrators will be conducted in Helsinki, Tallinn, and Barcelona.

From a technological perspective, it deploys (i) autonomous detection of IoT and AI threats, enriched with (ii) privacy-aware intelligence sharing and collaboration, and (iii) advanced data protection and accountability. Crucially, IRIS introduces (iv) the first dedicated online training and cyber exercises to prepare CERTs/CSIRTs to collaboratively protect critical infrastructures and systems against cross-border AI and IoT threats. IRIS will be validated in three pilot demonstrators, focussing in the IoT, AI and cross-border dimensions, across three existing smart city environments (in Helsinki, Tallinn and Barcelona), involving the associated national/governmental CERTs/CSIRTs, cybersecurity authorities and municipalities. The scenarios will contain real-life inspired cyber incidents that will build up into pilots at all levels (from local to national and to cross-border) to showcase the versatility of the IRIS solution. With 19 key partners from around Europe and 5 CERTs/CSIRTs as Associated Partners, IRIS's solid consortium composition and work plan prioritises the effectiveness needed for quick real-world adoption and impact. Moreover, integration will be carried out on the EU's existing MeliCERTes platform, with the support of INTRASOFT, while training will build upon THALES's existing cyber range, and ECSO will ensure the contribution to standards and policymaking. With the formal support of the four H2020 Cybersecurity Competence Network Pilot Projects, IRIS will also actively engage with the full scope of the cybersecurity ecosystem in Europe.

TAILOR

Project	TAILOR
Full Title	Foundations of Trustworthy AI - Integrating Reasoning, Learning and Optimization
GRANT AGREEMENT ID:	952215
Source of information	https://cordis.europa.eu/project/id/952215
EU contribution	€ 12 000 000 of a total costs : € 12 000 000
Coordinator	LINKOPINGS UNIVERSITET
Website:	http://www.liu.se/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999852236/952215





Funding Scheme	CP - Collaborative project (generic)
Start Date	1 September 2020
End Date	31 August 2023


The purpose of TAILOR is to build a strong academic-public-industrial research network with the capacity of providing the scientific basis for Trustworthy AI leveraging and combining learning, optimization and reasoning for realizing AI systems that incorporate the safeguards that make them in the reliable, safe, transparent and respectful of human agency and expectations. Not only the mechanisms to maximize benefits, but also those for minimizing harm. The network will be based on a number of innovative state-of-the-art mechanisms. A multi-stakeholder strategic research and innovation research roadmap coordinates and guides the research in the five basic research programs. Each program forming virtual research environments with many of the best AI researchers in Europe addressing the major scientific challenges identified in the roadmap. A collection of mechanisms supporting innovation, commercialization and knowledge transfer to industry. To support network collaboration TAILOR provides mechanisms such as AI-Powered Collaboration Tools, a PhD program, and training programs. A connectivity fund to support active dissemination across Europe through for example allowing the network to grow and to support the scientific stepping up of more research groups.

The project is ongoing. Many work products delivered by the project are available online for consultation:

Results

Table 16 Results of TAILOR project

1	A Dataset for Utility Prediction in Computational Persuasion with Machine Learning Techniques Author(s): Donadello, Ivan; Hunter, Anthony; Teso, Stefano; Dragoni, Mauro Published in: Zenodo	Dataset OpenAIRE  via
2	Videos from the paper "Best-of-N collective decisions on a hierarchy" Author(s): Vito, Trianni; Oddi Fabio; Andrea, Cristofaro Published in: Zenodo	Dataset OpenAIRE  via
3	Code, benchmarks and experiment data for the SoCS 2022 paper "Additive Pattern Databases for Decoupled Search" Author(s): Sievers, Silvan; Gnad, Daniel; Torralba, Álvaro Published in: Zenodo	Dataset OpenAIRE  via
4	Code and data for the SOCS 2022 paper "On Bidirectional Heuristic Search in Classical Planning: An Analysis of BAE*" Author(s): Kilian Hu; David Speck DOI: 10.5281/zenodo.6570805; 10.5281/zenodo.6570806 Publisher: Zenodo	Software OpenAIRE  via
5	Proofs, Code, and Data for the ICAPS 2022 Paper	Software OpenAIRE via

	Author(s): Dominik Drexler; Jendrik Seipp; Hector Geffner DOI: 10.5281/zenodo.6381592; 10.5281/zenodo.6381593 Publisher: Zenodo	
6	Recognizing LTLf/PLTLf Goals in Fully Observable Non-Deterministic Domain Models Author(s): Pereira, Ramon Fraga; Fuggitti, Francesco; De Giacomo, Giuseppe Published in: arxiv, 51, 2021 Publisher: Cornell University DOI: 10.48550/arxiv.2103.11692	Publication

AIDA

Project	AIDA
Full Title	Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies
GRANT AGREEMENT ID:	883596
Source of information	https://cordis.europa.eu/project/id/883596
EU contribution	€ 7 690 272,50 of a total costs : € 8 853 485
Coordinator	ENGINEERING - INGEGNERIA INFORMATICA SPA
Website:	http://www.eng.it/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999960488/883596
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2020
End Date	28 February 2023
Description of any problem encountered	

The EU-funded AIDA project is focusing on cybercrime and terrorism by approaching specific issues related to law enforcement agencies (LEAs) using pioneering machine learning and artificial intelligence methods. The project will deliver a descriptive and predictive data analytics platform and related tools which will prevent, identify, analyse and combat cybercrime and terrorist activities. The platform is based on the fundamental technology applied to Big Data analytics provided with AI and deep learning techniques expanded and tailored with additional crime-specific capabilities and tools. The system will be delivered to LEAs through a safe sandbox environment, improving the technological readiness level in operational conditions with real data.

The proposed solution aims to deliver a descriptive and predictive data analytics platform and related tools using state-of-the-art machine learning and artificial intelligence methods to prevent, detect, analyse, and combat criminal activities. AIDA will focus on cybercrime and terrorism, by addressing specific challenges

related to law enforcement investigation and intelligence. While cybercrime and terrorism pose distinct problems and may rely on different input datasets, the analysis of this data can benefit from the application of the same fundamental technology base framework, endowed with Artificial Intelligence and Deep Learning techniques applied to big data analytics, and extended and tailored with crime- and task- specific additional analytic capabilities and tools. The resulting TRL-7 integrated, modular and flexible AIDA framework will include LE-specific effective, efficient and automated data mining and analytics services to deal with intelligence and investigation workflows, extensive content acquisition, information extraction and fusion, knowledge management and enrichment through novel applications of Big Data processing, machine learning, artificial intelligence, predictive and visual analytics. AIDA system and tools will be made available to LEAs through a secure sandbox environment that aims to raise the technological readiness level of the solutions through their application in operational environment with real data.

3.6 Technology innovation

In the previous deliverable (D5.2) several projects were found to have interesting results in terms of available software or modelling. Among them, CONCORDIA and ECHO were moved to the section about cybersecurity, while others (INSIKT, ADABTS) were removed from the list because they appear not to be relevant anymore. By replicating the mapping on CORDIS Database, further ten interesting projects have been selected and added. The table below enlists these projects:

Table 17 Selected projects for technology innovation

acronym	title	start-end year	Mapped at
PLATFORMS and DATABASES			
CONNEXIONS	InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services	2018-2022	1 st search round
CounteR	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection	2021-2024	2 nd search round
TRAINING			
LAW-GAME	An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions	2021-2024	2 nd search round
CBRNE TECHNOLOGIES			
COSMIC	CBRNE Detection in Containers	2018-2021	1 st search round
INHERIT	INHibitors, Explosives and pRecursor InvesTigation	2021-2024	2 nd search round
ODYSSEUS	Preventing, Countering, And Investigating Terrorist Attacks Through Prognostic, Detection, And Forensic Mechanisms For Explosive Precursors	2021-2024	2 nd search round
PROACTIVE	PReparedness against CBRNE threats through cOMmon Approaches between security praCTitioners and the Vulnerable civil society	2019-2023	2 nd search round
TOOLS ABOUT MIGRATION			
CRiTERIA	Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks	2021-2024	2 nd search round

MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges	2018-2023	2 nd search round
OTHER			
DARLENE	Deep AR Law Enforcement Ecosystem	2020-2023	2 nd search round
TRAPEZE	TRAnsparency, Privacy and security for European citiZEns	2020-2023	2 nd search round
TechEthos	Ethics for Technologies with High Socio-Economic Impact	2021-2023	2 nd search round

Table 18 Selected projects for technology innovation

Below, the objectives and main results of these projects are reported. More specifically, an in-depth analysis of the newly mapped projects - 2nd search round - has been provided, while for the already mapped projects - 1st search round - the main focus was set on the latest updates and results achieved after the first round of mapping.

No updates were found for project COSMIC.

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
- 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.

The project was included in deliverable D5.2 and ended in early 2022. The project is interesting for NOTIONES with respect to both the focus area “*Technological needs, solutions, and improvements to the intelligence analysis phase of the Intelligence cycle*” and the focus area “*Improvements and Innovations to Various Intelligence Related Training*”. Two types of work products delivered by the project are currently available online for consultation: software and datasets.

Results

Table 19 Results of CONNEXIONS project

<p>Software via OpenAIRE</p> 	<p>First demonstrator of creation of BIM and GIS models for optimal surveillance & 3D scene reconstruction. Author(s): Nikolaos Patsiouras; Xenophon Zabulis DOI: 10.5281/zenodo.4432099; 10.5281/zenodo.4432100 Publisher: Zenodo</p>
<p>Datasets via OpenAIRE</p> 	<p>Two rooms connected by a corridor Author(s): Theodoros Evdemon; Xenophon Zabulis Published in: Zenodo</p> <p>Multimodal 3D Digitisation of a Simulated Crime Scene Author(s): Galanakis, George; Zabulis, Xenophon; Evdemon, Theodoros; Koutlemanis, Panagiotis Published in: Zenodo</p>

Counter

Project	Counter
Full Title	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection
GRANT AGREEMENT ID:	101021607
Source of information	https://cordis.europa.eu/project/id/101021607

EU contribution	€ 6 994 812,50 of a total costs : € 6 994 812,50
Coordinator	ASSIST SOFTWARE SRL
Website:	http://www.assist.ro/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/984731973/101021607
Funding Scheme	RIA – Research and Innovation action
Start Date	1 May 2021
End Date	30 April 2024

In order to support the fight against radicalization and thus prevent future terrorist attacks from taking place, the Counter project will bring data from diverse sources into an analysis and early alert platform for data mining and prediction of critical areas (e.g. communities), aiming to be a frontline community policing tool which looks at the community and its related risk factors rather than targeting and surveilling individuals. This is a key point in ensuring the privacy of citizens and the protection of their personal data, an issue that has been of great concern to policymakers and LEAs alike, who must balance the important work they do with the need to protect innocent individuals.

The system will incorporate state of the art NLP technologies combined with expert knowledge into the psychology of radicalization processes to provide a complete solution for LEAs to understand the when, where and why of radicalization in the community to help combat propaganda, fundraising, recruitment and mobilization, networking, information sharing, planning/coordination, data manipulation and misinformation. Information gained by the system will also allow LEAs and other community stakeholders to implement prevention programs and employ counternarratives rather than relying solely on surveillance. The Counter solution will cover a wide range of information sources, both dynamic (e.g. social media) and offline (e.g. open data sources) and combined with world-renowned expertise in radicalization processes and their psychology. The Counter solution will allow LEAs to take coordinated action in real-time while also preserving the privacy of citizens, as the system will target “hotspots” of radicalization rather than individuals.

In addition, the Counter solution will support information sharing between European LEAs and foster collaboration between diverse agencies by providing an open platform which prioritizes harmonized information formats.

The project is ongoing. No work products are available so far.

LAW-GAME

Project	LAW-GAME
Full Title	An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions
GRANT AGREEMENT ID:	101021714
Source of information	https://cordis.europa.eu/project/id/101021714
EU contribution	€ € 6 999 490 of a total costs : € € 6 999 490
Coordinator	EUROPEAN UNIVERSITY - CYPRUS LTD

Website:	http://www.euc.ac.cy/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999739619/101021714
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2021
End Date	31 August 2024

The EU-funded LAW-GAME project will use gamification technologies to train police officers on procedures in a safe and controlled virtual environment in Greece, Spain, Lithuania, Romania, and Moldova. The project will introduce an attractive method to develop competencies required to perform AI-assisted intelligence analysis and illegal acts prediction. LAW-GAME will conduct forensic examination through a one-player or multi-player cooperative scenario and provide developed AI tools for evidence recognition, crime scene investigation, and car accident analysis. The project will expose the trainees to police interview tactics and train them to recognise and mitigate potential terrorist attacks. The aim of our project is to train police officers' on the procedure, through gamification technologies in a safe and controlled virtual environment. Essential tasks during the creation of LAW-GAME serious game are to virtualise and accurately recreate the real world. We will introduce an attractive approach to the development of core competencies required for performing intelligence analysis, through a series of AI-assisted procedures for crime analysis and prediction of illegal acts, within the LAW-GAME game realm. Building upon an in-depth analysis of police officers' learning needs, we will develop an advanced learning experience, embedded into 3 comprehensive "gaming modes" dedicated to train police officers and measure their proficiency in:

1. conducting forensic examination, through a one-player or multi-player cooperative gaming scenario, played through the role of a forensics expert. Developed AI tools for evidence recognition and CSI and car accident analysis, will provide guidance to the trainee.
2. effective questioning, threatening, cajoling, persuasion, or negotiation. The trainee will be exposed to the challenges of the police interview tactics and trained to increase her emotional intelligence by interviewing a highly-realistic 3D digital character, advanced with conversational AI.
3. recognizing and mitigating potential terrorist attacks. The trainees will impersonate an intelligence analyst tasked with preventing an impending terrorist attack under a didactic and exciting "bad and good" multiplayer and AI-assisted game experience.

The project is ongoing and appears to be very interesting for NOTIONES with respect to the focus area "*Improvements and Innovations to Various Intelligence Related Training*".

INHERIT

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 FORSKNING SINSTITUT

	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

The EU-funded INHERIT project will develop a multidisciplinary approach to intervene across numerous stages of the terrorism timeline with a focus on explosive precursor chemicals. Specifically, it will develop technologies to render chemicals inert, more readily detectable and capable of yielding greater forensic value. The aim will be to make it impossible for terrorists to exploit these materials for the production of explosives.

The terrorism timeline consists of multiple stages. Each stage possesses vulnerabilities that can be used to disrupt a planned attack. Due to the large diversity in precursors, there is no universal approach yet that can be taken to keep a terrorist from using them to make explosives. INHERIT proposes to develop a multi-disciplined approach to intervene across multiple stages of the terrorism timeline. INHERIT has assembled a multi-faceted team with experience of all aspects of four important steps in this timeline. With a focus on explosive precursor chemicals, the team will work to develop technologies directed towards thwarting the ability of terrorists to exploit these materials for production of explosives. Methodologies to render chemicals inert, more readily detectable and capable of yielding greater forensic value will all be pursued. Collaboration between the diverse teams developing these interventions will ensure a coordinated holistic approach across all threat materials identified. This holistic approach will also be applicable in the struggle against emerging and future HME threats. The knowledge and insight resulting from INHERIT testing and analysis will be fed to targeted authorities, legislators, and organisations through a dissemination process which will include meetings, workshops and conferences conducted at appropriate security levels.

The project is ongoing. No work products are available so far.

ODYSSEUS

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	

ODYSSEUS project will develop effective and efficient prognostic, detection and forensic tools to improve prevention, countering and investigation of terrorist incidents involving home-made explosives. The knowledge will help in the development of tools for monitoring the chemical supply chain and sensing in (near) real-time explosive precursors. The tools will be field-tested in three operational use cases.

ODYSSEUS aims to increase the knowledge on explosive precursors and homemade explosives (HMEs), including precursors not previously studied, and develop effective and efficient prognostic, detection, and forensic tools to improve the capabilities of LEAs towards the prevention, countering, and investigation of terrorist incidents involving HMEs. ODYSSEUS will build upon relevant previous projects mainly HOMER, through the involvement of HOMER's core partners in this consortium, and will thus continue the work already done in HOMER on some precursors and further extend it to not previously studied precursors. To discover potentially hitherto unknown information, online HMEs recipes will be collected and their content will be analysed so as to extract knowledge about (possibly unknown) precursors and HMEs. Selected precursors will be then characterised and analysed for determining their explosive properties, feasibility, and potential for becoming a threat. This knowledge will be leveraged for developing tools for (i) chemical supply chain monitoring for irregularity detection to enable prediction and localisation of potential threats; (ii) advanced sensors for detecting in (near) real-time explosive precursors through air emissions and sewerage networks; (iii) robotised tools for improved mobile detection and in-situ forensic support; and (iv) automated threat detection, localisation, and assessment; these tools will be integrated into a configurable platform that will assist LEAs' operations in diverse scenarios.

ODYSSEUS will be validated in lab and field tests and demonstrations in three operational use cases. Extensive training of LEAs' personnel, hands-on experience, joint exercises, and training material will boost the uptake of ODYSSEUS tools and technologies.

The project is ongoing. No work products are available so far. The project is interesting for NOTIONES with respect to the focus area *"Improvements and Innovations to Various Intelligence Related Training"*.

PROACTIVE

Project	PROACTIVE
Full Title	PReparedness against CBRNE threats through cOmmon Approaches between security praCTitioners and the Vulnerable civil society
GRANT AGREEMENT ID:	832981
Source of information	https://cordis.europa.eu/project/id/832981

EU contribution	€ 4 970 028,75of a total costs : € 4 970 028,75
Coordinator	UNION INTERNATIONALE DES CHEMINS DE FER
Website:	http://www.uic.org/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999738649/832981
Funding Scheme	RIA - Research and Innovation action
Start Date	1 May 2019
End Date	31 July 2023

In line with the EU Action Plan to enhance preparedness against chemical, biological, radiological and nuclear (CBRN) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aims to enhance societal CBRN preparedness by increasing Practitioner effectiveness in managing large, diverse groups of people in a CBRN environment. This will be achieved by testing common approaches between European Practitioners such as Law Enforcement Agencies (LEAs) and First Responders. These will be evaluated and validated against the requirements of civil society, including vulnerable groups of citizens reflected in the European Security Model. A Practitioner Stakeholder Advisory Board and a Civil Society Advisory Board will extend the representation of both sides in several surveys, focus-groups, workshops and field exercises. A benchmark study between LEAs will identify common approaches in assessing CBRN threats and the protocols and tools used to help citizens. Liaising with the eNOTICE H2020 project, three joint exercises will include role play volunteers recruited by PROACTIVE. They will evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE to provide innovative recommendations for Policy-makers and safety and security Practitioners.

PROACTIVE will result in toolkits for CBRN Practitioners and for civil society organisations. The toolkit for Practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a mobile app. The toolkit for the civil society will include a mobile app adapted to various vulnerable citizen categories and pre-incident public information material. These will provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRN activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats.

The project is ongoing. Many work products delivered by the project are available online for consultation:

Results

Table 20 Results of PROACTIVE project

1	Guidelines and recommendations for mitigation and management of CBRNe terrorism	Report
2	Report on the High-level Architecture design including an interface control document	Report
3	Requirements of the Mobile App for vulnerable citizens and revised technical specifications	Report
4	Findings from systematic review of public perceptions and responses	Report
5	CBRNe and vulnerable citizens: co-creating an app for that Author(s): Laura Petersen, Grigore Havarneanu, Garik Markarian, Natasha McCrone	Publication

Published in: 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 2019, 2020, Page(s) 1 - 4, ISBN 978-1-7281-4920-2	
Publisher: IEEE	
DOI: 10.1109/ict-dm47966.2019.9032967	

CRITERIA

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

The EU's external borders are busy places. Border officials are required to address numerous issues – from document fraud and public health threats to people smuggling, unregulated migration and terrorism. In this context, the EU-funded CRITERIA project will design a risk assessment methodology that stems from existing analysis technologies and tools that are tailored to the new comprehensive threat indicators of its methodology. The focus will be on the role of narratives, events and attitudes and the vulnerability of borders and humans. Bringing together an interdisciplinary team of experts, CRITERIA's methodology will be developed with input from practitioners from border agencies.

The CRITERIA project will develop a novel risk analysis methodology, which is, on the one hand, clearly rooted and builds upon existing methodology such as CIRAM and, on the other hand introduces novel more complex and effective indicators, which overcome important limitations of existing models. Such extended risk and vulnerability analysis methodology has to be backed by effective intelligent analysis technology. Building upon existing text, media, data and network analysis technology, CRITERIA, will develop and evaluate advanced analysis technologies and tools that are tailored to the new comprehensive threat indicators of the CRITERIA methodology. Special focus will be put to the consideration of the role of narratives, events, attitudes, and to the vulnerability of borders and humans as well as on providing semi-automatic tools and methods for risk-related evidence validation and explanation, for identifying risk propagation and interlinking, thus supporting decision processes in risk analysis in an innovative way. When developing this holistic CRITERIA risk and vulnerability analysis framework for border agencies ethical, legal and societal aspects will be considered from the very beginning. The methodology will be developed in close collaboration

with practitioners from border agencies, which will also validate the developed methods and technologies in piloting activities.

The project was included in deliverable D5.2 and it is ongoing. No work products delivered by the project are available online so far.

MEDEA

Project	MEDEA
Full Title	Mediterranean practitioners' network capacity building for effective response to emerging security challenges
GRANT AGREEMENT ID:	787111
Source of information	https://cordis.europa.eu/project/id/787111
EU contribution	€ 3 495 843,75 of a total costs : € 3 495 843,75
Coordinator	KENTRO MELETON ASFALIAS
Website:	http://www.kemea.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999827307/787111
Funding Scheme	IA – Innovation Action
Start Date	1 June 2018
End Date	31 May 2023

The MEDEA project, during its 60 months of implementation provides funding for four interrelated actions:

- i. Establish and Operate the MEDEA network, a multi-disciplinary network of security practitioners, with active links to policy makers and users/providers of security innovations across the M&BS countries focusing in Border Protection and other Security- and Disaster-Related tasks. During the project duration, MEDEA members will engage in activities towards maintaining its sustainability and longevity after the financing of this project ends,
- ii. Engage participants in anticipatory governance on emerging security challenges that the Mediterranean and Black Sea regions would face in the coming years (present until +10 years), which concretely operationalizes the backbone of the project in a triple structure: a) understanding unsatisfactory state of play, b) design the desirable future and c) define a resilient pathway on how to achieve this,
- iii. Push for the “co-creation” of security technology and capabilities innovations between practitioners and innovation suppliers, which is based upon their evaluation and prioritization on multi-criteria analysis (technology, operational and cost-benefit, etc.) and also linked to Human Development, Policy Making and Organizational Improvements in-terms of facilitating its use by the practitioners
- iv. Establish and annually update the Mediterranean Security Research and Innovation Agenda (MSRIA), that identifies areas where security & defence research is needed and the establishment of recommendations for European Security & Defence technology investments.

The project is ongoing. Many work products delivered by the project are available online for consultation:

Results

Table 21 Results of MEDEA project

1	MEDEA collaboration platform	Platform
2	Database of cross border crime TCP scenarios	Database
3	Database of Disaster Resilient Scenarios	Database
4	Database of Border management and surveillance Scenarios	Database
5	Database of Migration Management Scenarios	Database
6	Mediterranean Research and Innovation Agenda v2	Report

DARLENE

Project	DARLENE
Full Title	Deep AR Law Enforcement Ecosystem
GRANT AGREEMENT ID:	883297
Source of information	https://cordis.europa.eu/project/id/883297
EU contribution	€ 6 954 860 of a total costs : € 6 954 860
Coordinator	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS
Website:	http://www.certh.gr/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/998802502/883297
Funding Scheme	RIA – Research and Innovation action
Start Date	1 September 2020
End Date	31 August 2023

DARLENE aims to investigate means by which Augmented Reality (AR) can be deployed in real time to aid in LEA decision-making by employing AR capabilities and combining them with powerful ML algorithms, sensor information fusion techniques, 3D reconstruction, wearable technology and personalized context-aware recommendations. Hence DARLENE will offer European LEAs a proactive security solution which will provide an IoT level of Situational Awareness, detection and recognition, combining cutting edge technology and public security in all security verticals. It will enable LEAs to reduce and prevent crime, and to more quickly respond to crimes already in progress, by enabling them to sort through massive volumes of data to predict, anticipate and prevent criminal activities, make better informed tactical decisions and provide enhanced protection services for European citizens. DARLENE will therefore develop practical and beneficial policing applications through the use of affordable, light-weight and inconspicuous AR glasses. Such applications will capitalize on cutting edge research that will combine with AR Technology to create innovative methods for combating crime and even terrorist acts.

To align technology development with actual security needs and requirements, DARLENE will build a community of LEAs organization and security stakeholders that will guide the development process and evaluate the entire DARLENE ecosystem. In this regard, DARLENE foresees extensive demonstration and training activities for LEAs while the entire solution will be demonstrated and validated in realistic scenarios during the pilot phase of the project, thus paving the way to its field deployment and commercial uptake.

The project is ongoing. The project is interesting for NOTIONES with respect to the focus area “*Improvements and Innovations to Various Intelligence Related Training*”. Many work products delivered by the project are available online for consultation:

Results

Table 22 Results of DARLENE project

1	DARLENE platform handbook and tutorial content - 1st version	Interactive application
2	<p>DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions</p> <p>Author(s): Konstantinos C. Apostolakis; Nikolaos Dimitriou; George Margetis; Stavroula Ntoa; Dimitrios Tzovaras; Constantine Stephanidis; Constantine Stephanidis</p> <p>Published in: Open Research Europe, 1, 2022, ISSN 2732-5121</p> <p>Publisher: Directorate-General for DG RTD</p> <p>DOI: 10.12688/openreseurope.13715.1</p>	Publication
3	<p>Real-Time Stress Level Feedback from Raw Ecg Signals for Personalised, Context-Aware Applications Using Lightweight Convolutional Neural Network Architectures</p> <p>Author(s): Konstantinos Tzevelekakis; Zinovia Stefanidi; George Margetis</p> <p>Published in: Sensors (Basel, Switzerland), 1, 2021, Page(s) 7802, ISSN 1424-8220</p> <p>Publisher: Multidisciplinary Digital Publishing Institute (MDPI)</p> <p>DOI: 10.3390/s21237802</p>	Publication
4	<p>Real-Time Adaptation of Context-Aware Intelligent User Interfaces, for Enhanced Situational Awareness</p> <p>Author(s): Z. Stefanidi, G. Margetis, S. Ntoa and G. Papagiannakis</p> <p>Published in: IEEE Access, 10, 2022, Page(s) 23367-23393, ISSN 2169-3536</p> <p>Publisher: Institute of Electrical and Electronics Engineers Inc.</p> <p>DOI: 10.1109/access.2022.3152743</p>	Publication

TRAPEZE

Project	TRAPEZE
Full Title	TRANsparency, Privacy and security for European citiZEns
GRANT AGREEMENT ID:	883464
Source of information	https://cordis.europa.eu/project/id/883464
EU contribution	€ 4 995 812,50 of a total costs : € 6 017 950
Coordinator	TENFORCE
Website:	https://www.tenforce.com/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/985890347/883464
Funding Scheme	IA - Innovation action
Start Date	1 September 2020
End Date	31 August 2023

The TRAPEZE project aims to drive a cultural shift in the protection of the European data economy by weaving trust into its very foundation and reconstructing the concepts of control, transparency, and compliance through technical and methodological, citizen-first, innovations. Driven by the needs of three distinct real-world use cases, TRAPEZE brings together over a decade worth of EU-funded research in security and privacy, as well as proprietary solutions and know-how, towards realistic and marketable solutions. We will develop technologies which: (i) empower citizens with the necessary tools and know-how to manage their security and privacy and actively contribute to the cyber resilience of the common European data space; (ii) enforce the integrity and nonrepudiation of citizens' data usage policies and processing across data sources and controllers' borders; (iii) dynamically acquire citizens' consent and adjust their data policies in real time in response to their changing circumstances; (iv) protect citizens' online communications and applications running on their personal devices against malicious agents; and (v) provide citizens, as well as other relevant stakeholders (including controllers, CERTs/CSIRTs, and data protection authorities) with a comprehensible overview of transborder data lineage and flows, as well as proof of legal compliance, even in big data environments. By relying on Linked Data and Blockchain, TRAPEZE will lead the way in putting the often-misplaced cutting-edge technologies to practical use and become a lighthouse for European and global initiatives aiming to deliver privacy-aware innovations. Finally, to ensure citizens of all groups can have an active role in the protection of their data flows, TRAPEZE will place a special emphasis on usability and co-production, involving European citizens directly in the development of its security- and privacy-enhancing technologies.

The project is ongoing. Many work products delivered by the project are available online for consultation:

Results

Table 23 Results of TRAPEZE projects

1	TRAPEZE Security and Data Protection knowledge base - First version	Report
2	TRAPEZE platform - First version	Platform
3	Real-time reasoning in OWL2 for GDPR compliance Author(s): Piero A. Bonatti, Luca Ioffredo, Iliana M. Petrova, Luigi Sauro, Ida R. Siahann,	Publication

	Published in: Artificial Intelligence, 2020, Page(s) Volume 289,, ISSN 0004-3702 Publisher: Elsevier BV DOI: 10.1016/j.artint.2020.103389	
4	Security and Privacy Resilience Framework and Guidelines - Second version	Report

TechEthos

Project	TechEthos
Full Title	Ethics for Technologies with High Socio-Economic Impact
GRANT AGREEMENT ID:	101006249
Source of information	https://cordis.europa.eu/project/id/101006249
EU contribution	€ 3 994 592,50 of a total costs : € 3 994 592,50
Coordinator	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
Website:	http://www.ait.ac.at/
Coordinator Contact:	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/contact-form/PROJECT/999584128/101006249
Funding Scheme	CSA – Coordination and Support action
Start Date	1 January 2021
End Date	31 December 2023

TechEthos will reinforce the pivotal role of the European Union as an ethics trailblazer in new and emerging technologies. Such technologies bring with them new ethical challenges and societal consequences that need to be addressed. The project will develop guidance for the development and deployment of these technologies to ensure the highest ethical standards at the EU and international levels. It will carry out a horizon scan to identify three or four new technologies with high socio-economic impact. It will then identify and analyse the ethical issues raised by the selected technologies and explore the views and attitudes of expert and lay stakeholders towards them and their ethical implications using scenarios and media analysis. Public involvement is key in this project: science museums and centers involved in our work will ensure appropriate TechEthos will address the growing ethical challenges and expectations vis-à-vis new technologies to ensure the highest ethical standards at the EU and international levels. It will conduct a horizon scan of emerging technologies with high socio-economic impacts to identify 3-4 that may raise particularly challenging ethical issues; these will be further analysed and engaged with in the project (via ethical and legal analysis and stakeholder engagement activities). The project will develop/refine/extend (as desirable and applicable to the selected technologies) existing/proposed ethics frameworks, operational guidelines or Codes (e.g. developed in SIENNA, SHERPA, PANELFIT, SATORI and other projects) to enable the effective ethics governance of the technologies. It will reconcile the needs of research and innovation and the legitimate concerns of the society while stimulating innovation and reducing socio-economic inequalities. To do so, it will especially engage with researchers and innovators, research ethics committees (RECs), research integrity (RI) bodies, civil society organisations (CSOs), policy-makers and the public.

The project is ongoing. Two publications delivered by the project are available online for consultation:

Results

Table 24 Results of TechEthos project

1	<p>Ethics of Climate Engineering: Don't forget technology has an ethical aspect too</p> <p>Author(s): Laurence Brooks, Sara Cannizzaro, Steven Umbrello, Michael J. Bernstein & Kathleen Richardson</p> <p>Published in: International Journal of Information Management, 2021, ISSN 0268-4012</p> <p>Publisher: Pergamon Press Ltd.</p> <p>DOI: 10.1016/j.ijinfomgt.2021.102449</p>	Publication
2	<p>Thinking AI with a hammer. Kate Crawford's Atlas of AI (2021)</p> <p>Author(s): Anais Resseguier</p> <p>Published in: AI and Ethics, 2022, Page(s) 247-248, ISSN 2730-5961</p> <p>Publisher: Springer</p> <p>DOI: 10.1007/s43681-021-00115-7</p>	Publication

4. Follow-up of recommendations from WP6

WP5 also took responsibility of the follow-up of recommendations provided by previous tasks and Work Packages, providing updated information on:

- research projects and technologies considered relevant by the NOTIONES practitioners in WP6;
- topics tackled in WP3 that needed further investigation.

In the next subsections, the results of these follow-up activities are presented.

4.1 T6.1 recommendations

NOTIONES Work Package 6 “Interaction between practitioners and other stakeholders” organized the first round of Working Groups in task T6.1. Here, the practitioners were able to review the technologies and research projects proposed by WP3 and WP5 and they voted them based on their potential.

Those voted as relevant by at least two thirds of the practitioners in the WG – so at least 3 out of 4 in WG1 and at least 2 out of 3 in WG2⁶ - are reported below in Table 25, with those voted by 100% of the practitioners in the WG highlighted in bold:

RESEARCH PROJECTS		
source	voted by WG1	voted by WG2
D5.2	TITANIUM, DAN, CONNEXIONS	PREVISION, INFINITY*, TRACE*, SiiP, CONCORDIA, ECHO, CONNEXIONS, ADABTS
D3.6	AIDA*, WILDTRADE, Anti-FinTer, INSIGHT, ISF ProFID	AIDA*, CTC, STARLIGHT*, GRACE, INFINITY, INSPECT, SIGNIFICANCE, ENFORCE, INSIGHT
D3.5	ASGARD, ANITA, CONNEXIONS, PREVISION, BIGOSINT	AIDA*, BIGOSINT, CONCORDIA, CONNEXIONS, COPKIT, DARE, PAPAYA, SPARTA, SceMaps
TECHNOLOGIES and TOOLS		
source	voted by WG1	voted by WG2
D3.6	<p><i>Face recognition:</i> Amazon Rekognition, Betaface, Prum II</p> <p><i>Child sexual exploitation detection:</i> Childsafe.ai, Griffey, Aviator</p> <p><i>Cryptocurrency investigation:</i> Chainanalysis, CIPHERTRACE, QLUE, Cellebrite Crypto Tracer</p>	<p><i>Face recognition:</i> BetaFace, BioID, Cognitec FaceVACS-DBScanLE, Prum II</p> <p><i>Child sexual exploitation detection:</i> Childsafe.ai, SpotLight, Griffey, 4NSEEK, Aviator</p> <p><i>Video surveillance based crime detection:</i> Flock Safety’s Falcon, Axon, OpenAFIS</p>

⁶ Working Group 1, dedicated to “Various challenges to monitoring and collecting data from the darknet” saw the participation of four practitioners (KWPR, MAGMA, DANS and FIU) while Working group 2, dedicated to “Technological needs, solutions and improvements to the analysis phase of the Intelligence cycle” saw the participation of 3 practitioners (EPBJ, PJ and KhnUIA)

		<p><i>Cryptocurrency investigation:</i> Chainanalysis, Ciphertrace, QLUE, Cellebrite Crypto Tracer</p> <p><i>Crime prevention:</i> PRECOBS, VeriPol, VALCRI, HART</p> <p><i>Digital forensics automation:</i> Magnet Digital Investigation Suite, Exterro FTK</p>
D3.3	<p><i>Digital Forensics automation:</i> Darkowl, Cybersixgill, Group-IB, Maltego, IBM i2/i2 Group, Cellebrite, Cobwebs Technologies, Constella Intelligence, Blackdot Solutions, KELA, Web-IQ</p>	<p><i>Illegal traffic detection:</i> iARMS**, Targeton Trafficking, Entrupy</p> <p><i>Digital forensics automation:</i> DarkOwl, Cybersixgill, Group-IB, Flashpoint, Cobwebs Technologies, SS8 Networks, Web-IQ, Intel 471</p>
D3.5	<p><i>NLP solutions:</i> Deep Pavlov, SpaCy</p> <p><i>Data Scraping Solutions:</i> Apache Nutch, Heritrix, Scrapy, Selenium, JSOUP, the Apache POI</p>	<p><i>NLP solutions:</i> SpaCy</p>

Table 25 Research projects and technologies/tools voted by WG1 and WG2

In bold those voted by 100% of practitioners in each Working Group. *practitioners already inside this projects **already extensively used by all LEAs

Research projects and technologies/tools that gained more votes in the WGs deserved further deepening and possibly interaction: WP5 took care of this, in close cooperation with WP8.

In regard of the research projects, partners contributing in WP5 made every effort to contact the coordinators and ask for more detailed information on the projects’ outcomes and relevance for NOTIONES. In selected cases - AIDA, ANITA, ECHO, INFINITY, and CTC - it was possible to obtain consistent information about the innovation potential of the projects and a collaboration was started within the NOTIONES network. Contacts with PREVISION, INSPECTr, PopAI and ALIGNER projects were also successful. The remaining projects are still in the process of being contacted within WP5 and WP8. The main innovations are described in section 4.1.1.

Little information was found about the technologies and tools voted by the practitioners, apart from what is already available online in the technology providers’ websites. All partners contributing in the activities of WP5 contacted assigned technology providers repeatedly, asking for information about the functionalities of their products, the pricing etc. and the availability of demonstrative or informative material. WP5 tried to contact the providers of the following technologies: AviaTor, BetaFace, Cellebrite Crypto Tracer, Cybersixgill, Group-IB, QLUE, Web-IQ.

In most cases, there was no answer. Only BetaFace answered, but they did not provide any material or information – despite this, at least they answered and the communication channel is still open, so section 4.1.2 some additional insights on this technology is provided, based on open information. Positive feedback and availability to organize demos was obtained only for technology providers with direct contacts in real life with partners of the NOTIONES consortium: CobWeb Technologies, QLUE, Datawalk and XRI MSAB, that all have direct contacts with TECOMS. In addition to these, also IPS-Intelligence and OSINT Analytics were

successfully contacted by SYNYO, provided informative material and gave availability for presenting their products to NOTIONES.

Technology providers may be more prone to answer contact requests made directly by practitioners. It is also possible that they use other channels to find potential customers, such as trade shows and specialized events, instead of direct contact. This is a big issue that must be carefully discussed in NOTIONES, so that a good strategy can be planned towards the risk of not being able to reach technology providers.

4.1.1 Research projects

For projects AIDA and ANITA it was possible to obtain information on the innovation potential of the Natural Language Processing (NLP) solutions developed by the projects in close cooperation with Law Enforcement Officers. This is a practical example of how the strong involvement of end-users can provide real added value to EU-funded security projects and contribute to the advancement of technology.

AIDA innovations in NLP

The AIDA project domain is composed of two main areas that are Cyber Crime (CC) and Counter Terrorism (CT).

Text analytics services are identified to extract (I) the most relevant categories according to relevant taxonomies (intelligence, crime, terrorism, cybercrime, emotions); (II) entities (people, places, organizations, dates, criminal organizations, malware, etc.); (III) main sentences; (IV) main word(groups). Then, the results of these extraction process will be exploited for AI Machine Learning based algorithms that will be used to automatically assist LEAs in the analysis of the collected datasets and alerting in case of suspicious events.

Regarding the CT scenario (Deployment of AIDA's Analytical Features), analysts should analyse the text and extract detailed narrative analysis and other entities that will be provided to Member States. Text analysis tools are identified to provide (I) summarisation: main sentences, main words; (II) entity extraction: entities mentioned in the transcript of the audio such as people, organizations and places (also, domain-specific entities such as terrorist organizations, critical infrastructures); (III) classification: identify main topics in the text and which sentences contributed to those topics based on existing taxonomies for intelligence, terrorism and terrorist narratives (based on a e.g. idealizing martyrs, discrediting competing groups); (IV) find and suggest links to similar documents for relevant sentences in the text; (V) produce a stylometric profile for a specific user and try to predict sociodemographic attributes of the author (e.g. age range, educational level, gender).

State of the art of NLP

As reported in NOTIONES D3.5, the state of the art of NLP processes, before AIDA innovations, can be summarized with the following:

- Text subdivision (atoms, tokens, phrase, sentences, paragraphs);
- Part-of-speech tagging (POS);
- Morphological analysis;
- Lemmatization;
- Syntactic analysis (sentence structure, universal dependency relation);
- Semantic analysis (word sense disambiguation);

- Key elements identification (relevant topics, main sentences, main phrases, main concepts and main lemmas);
- Name entity recognition (NER);
- Entity relations (semantic role labelling), sentiment analysis.
- Media topics;
- Geography;
- Emotional
- Behavioural traits.
- Taxonomies: Cyber Crime, Terrorism, Radicalization Narratives, Crime, Intelligence, Geography, Emotions

AIDA NLP Innovations

For the Text Analysis Tools, AIDA project is developing improvements to core technology stack presented in the previous section. Regarding the *Deep Learning Techniques*, it has chosen a specific Transformers architecture called Adapter Transformers. This modular architecture allows to use several task-oriented trained models into a single instance, saving memory and reducing computational costs. This architecture leverages a big single neural network model as basis and stacks on top different lightweight modules named adapters. Each adapter is generally composed of a two-layer feed-forward neural network trained for a single downstream categorization or regression task. This alternative to a fully model fine-tuning allows to preserve the integrity of the base model, preventing catastrophic forgetting and facilitating transfer learning and knowledge compositionality.

The core of *Text Analytics* is based on expert.ai tools written with proprietary programming languages and Java⁷. *Text Encoding* have been developed using Python⁸ as programming language, even though part of the stylometric text encoding is based on expert.ai stylometric feature extraction tool.

Text Classification Tool

Text Classification or text categorization is the process of grouping documents into classes or categories. Together with the existing taxonomies, the AIDA project has built enhancements regarding the Cybercrime (CC) and Terrorism (CT) taxonomies. They are carried out from a specific work that has involved also LEA partners involved in the project and improved with customized modifications that were requested. These changes are listed and described in the next subsection.

The cooperation with LEAs during the AIDA workshop on taxonomies resulted into a list of changes and improvements designed to provide a tailored categorization for the project needs. The comparison of taxonomies before and after the changes is presented in Table 26 for Cybercrime taxonomy and Table 27 for Terrorism taxonomy. The list of the specific changes is reported below:

- Split the pre-existing “left wing and anarchist terrorism and extremism” category into the two “left wing terrorism and extremism” and “anarchist terrorism and extremism” new categories.
- Added the new categories “Arson”, “Fire”, “Slaughtering”, “Execution” as sub-categories of “Terrorist activities and tactics”.
- Added the new category “Inghimasi” as sub-category of “Guerrilla”, and “Inghimasi suicide bombing” as sub-category of “Suicide bombing”
- Added the new categories “terrorist attack on hospitals”, “terrorist attack on media stations”, “terrorist attack on border controls” as sub-categories of “Terrorist attack on public building”

⁷ <https://github.com/openjdk/>

⁸ <https://github.com/python>

- Added the new categories “Ransom” and “Reward” as sub-categories of “Terrorism organizational model”.
- Added the new categories “Terrorist attack on writers”, “Terrorist attack on journalists”, “Terrorist attack on judges”, “Terrorist attack on minorities” as sub-categories of “Terrorist attack on civilians and properties”.
- Added the categories “Terrorist attack on LGBTs”, “Terrorist attack on “Christians”, “Terrorist attack on Muslims”, “Terrorist attack on Jews” as sub-categories of the new “Terrorist attack on minorities” category.
- Split the pre-existing “Recruitment and training” category into the two “Recruitment” and “Training” new categories.
- Split the pre-existing “Propaganda and ideology” category into the two “Propaganda” and “Ideology” new categories.
- Added “Cyber criminals offering cyber-crime-as-a-service” as sub-category of “Cyber criminals”

Table 26 Cybercrime Taxonomy comparison before and after changes

Old Cybercrime Taxonomy	New Cybercrime Taxonomy
<ul style="list-style-type: none"> ● Cyber Attack <ul style="list-style-type: none"> ○ DoS attack ○ Intrusion (computer or network) <ul style="list-style-type: none"> ▪ Defacing ▪ Account compromised ▪ Data dump/Data loss ○ Interception attack ○ Injection ○ Cross-site scripting ○ Cross-site request forgery ○ Broken authentication and session management ○ Man-in-the-middle ● Cyber deception <ul style="list-style-type: none"> ○ Information gathering <ul style="list-style-type: none"> ▪ Identity theft ▪ Phishing ○ Credit card fraud <ul style="list-style-type: none"> ▪ Skimming ○ Email spamming ○ Scam ● Cyber Violence ● Content-related Computer Crime <ul style="list-style-type: none"> ○ Cyber piracy ● Cyber criminals ● Cyber Security <ul style="list-style-type: none"> ○ Vulnerabilities <ul style="list-style-type: none"> ▪ Mobile vulnerability ▪ Application and software vulnerability ▪ Firmware vulnerability ▪ Zero-day ○ Threat and vectors <ul style="list-style-type: none"> ▪ Malware and virus ▪ Botnet ▪ Advanced Persistent Threat 	<ul style="list-style-type: none"> ● Cyber Attack <ul style="list-style-type: none"> ○ DoS attack ○ Intrusion (computer or network) <ul style="list-style-type: none"> ▪ Defacing ▪ Account compromised ▪ Data dump/Data loss ○ Interception attack ○ Injection ○ Cross-site scripting ○ Cross-site request forgery ○ Broken authentication and session management ○ Man-in-the-middle ● Cyber deception <ul style="list-style-type: none"> ○ Information gathering <ul style="list-style-type: none"> ▪ Identity theft ▪ Phishing ○ Credit card fraud <ul style="list-style-type: none"> ▪ Skimming ○ Email spamming ○ Scam ● Cyber Violence ● Content-related Computer Crime <ul style="list-style-type: none"> ○ Cyber piracy ● Cyber criminals <ul style="list-style-type: none"> ○ <u>Cyber criminals offering cyber-crime-as-a-service</u> ● Cyber Security <ul style="list-style-type: none"> ○ Vulnerabilities <ul style="list-style-type: none"> ▪ Mobile vulnerability ▪ Application and software vulnerability ▪ Firmware vulnerability ▪ Zero-day ○ Threat and vectors <ul style="list-style-type: none"> ▪ Malware and virus

<ul style="list-style-type: none"> <ul style="list-style-type: none"> ▪ Ransomware ○ Security software and devices • Cyber Terrorism • Cyber Espionage • Hacktivism • Malicious devices 	<ul style="list-style-type: none"> <ul style="list-style-type: none"> ▪ Botnet ▪ Advanced Persistent Threat ▪ Ransomware ○ Security software and devices • Cyber Terrorism • Cyber Espionage • Hacktivism • Malicious devices
--	--

Table 27 Terrorism Taxonomy comparison before and after changes

Old Terrorism Taxonomy	New Terrorism Taxonomy
<ul style="list-style-type: none"> • Terrorism by matrix <ul style="list-style-type: none"> ○ Religiously inspired ○ Ethno-nationalist and separatist ○ Left-wing and anarchist ○ Right-wing ○ Narco-terrorism ○ Eco-terrorism • Terrorist activities and tactics <ul style="list-style-type: none"> ○ Bombing <ul style="list-style-type: none"> ▪ Suicide bombing ▪ Roadside bombing ▪ Car bombing ○ Assassination ○ Hijacking and skyjacking ○ Kidnapping and hostage taking ○ Hostage murder ○ Armed attack (generic) ○ Mass violence <ul style="list-style-type: none"> ▪ Ethnic cleansing ▪ Mass expulsion ▪ Mass killings ○ Maritime Terrorism ○ Mass Transit Terrorism ○ Guerilla ○ Chemical attack ○ Biological attack ○ Radiological or nuclear attack ○ CBNR attack • Terrorism organization model <ul style="list-style-type: none"> ○ Propaganda and ideology ○ Recruitment and training ○ Terrorism financing ○ Political support to terrorism • Weapons <ul style="list-style-type: none"> ○ Weapons of mass destruction ○ Arsenals ○ IED and VBIED • Terrorist attacks by targets <ul style="list-style-type: none"> ○ on critical infrastructures <ul style="list-style-type: none"> ▪ on water supplies 	<ul style="list-style-type: none"> • Terrorism by matrix <ul style="list-style-type: none"> ○ Religiously inspired ○ Ethno-nationalist and separatist ○ <u>Left-wing terrorism and extremism</u> ○ <u>Right-wing terrorism and extremism</u> ○ Narco-terrorism ○ Eco-terrorism ○ <u>Anarchist terrorism and extremism</u> • Terrorist activities and tactics <ul style="list-style-type: none"> ○ Bombing <ul style="list-style-type: none"> ▪ Suicide bombing <ul style="list-style-type: none"> • <u>Inghimasi suicide bombing</u> ▪ Roadside bombing ▪ Car bombing ○ Assassination ○ Hijacking and skyjacking ○ Kidnapping and hostage taking ○ Hostage murder ○ Armed attack (generic) ○ Mass violence <ul style="list-style-type: none"> ▪ Ethnic cleansing ▪ Mass expulsion ▪ Mass killings ○ Maritime Terrorism ○ Mass Transit Terrorism ○ Guerilla <ul style="list-style-type: none"> ▪ <u>Inghimasi</u> ○ Chemical attack ○ Biological attack ○ Radiological or nuclear attack ○ CBNR attack ○ <u>Arson</u> ○ <u>Fire</u> ○ <u>Execution</u> ○ <u>Slaughtering</u> • Terrorism organization model <ul style="list-style-type: none"> ○ <u>Propaganda</u> ○ <u>Ideology</u> ○ <u>Recruitment</u> ○ <u>Training</u>

<ul style="list-style-type: none"> <ul style="list-style-type: none"> ▪ on oil production and distribution ▪ on electrical grid ▪ on public building ○ on NGO's, aid worker and contractors ○ on politicians or political or government institution ○ on diplomats or diplomatic institution ○ on civilians and properties ○ on religious leader or institution ○ on military and police forces and structures • Critical events and threats <ul style="list-style-type: none"> ○ Rebellions ○ Dissent, demonstration, disorders ○ Left-wing and anarchist extremist activities ○ Right-wing extremist activities • Counterterrorism <ul style="list-style-type: none"> ○ Institutions working against terrorism ○ Counterterrorism operations ○ Disarmament and demobilizations ○ Legal measure ○ Political initiatives ○ Financial support initiatives 	<ul style="list-style-type: none"> ○ Terrorism financing ○ Political support to terrorism ○ <u>Ransom</u> ○ <u>Reward</u> • Weapons <ul style="list-style-type: none"> ○ Weapons of mass destruction ○ Arsenals ○ IED and VBIED • Terrorist attacks by targets <ul style="list-style-type: none"> ○ on critical infrastructures <ul style="list-style-type: none"> ▪ on water supplies ▪ on oil production and distribution ▪ on electrical grid ▪ on public building <ul style="list-style-type: none"> • <u>on media station</u> • <u>on hospital</u> • <u>on border controls</u> ○ on NGO's, aid worker and contractors ○ on politicians or political or government institution ○ on diplomats or diplomatic institution ○ on civilians and properties <ul style="list-style-type: none"> ▪ <u>on writers</u> ▪ <u>on journalists</u> ▪ <u>on judges</u> ▪ <u>on minorities</u> <ul style="list-style-type: none"> • <u>on LGBTs</u> • <u>on Christians</u> • <u>on Muslims</u> • <u>on Jews</u> ○ on religious leader or institution ○ on military and police forces and structures • Critical events and threats <ul style="list-style-type: none"> ○ Rebellions ○ Dissent, demonstration, disorders ○ Left-wing and anarchist extremist activities ○ Right-wing extremist activities • Counterterrorism <ul style="list-style-type: none"> ○ Institutions working against terrorism ○ Counterterrorism operations ○ Disarmament and demobilizations ○ Legal measure ○ Political initiatives ○ Financial support initiatives
--	--

Text Encoding

Machine Learning algorithms need some sort of mathematical objects to process data through complex operations. In recent decades, various techniques have been developed to convert textual data into numerical representations (embeddings) that can be processed by machine learning algorithms such as *vector space models* like *bag of words* or *TFIDF (term frequency – Inverse document frequency)*. The most

advanced techniques to represent words and their compositionality are the so-called *Language Models* [25] that leverage artificial neural networks [4]. In recent years, the *Transformers* [5] architecture has rapidly become the cutting-edge technique for representing textual data. These kinds of representations can model deep linguistic properties leveraging big amount of data and unsupervised or semi-supervised machine learning techniques. Despite of the astonishing capabilities and performance obtained by these Language Models, frequently these representations lack domain specific knowledge and need to be fine-tuned for specific classification or regression tasks.

This section presents the specific models selected to represent (encode) textual data and the techniques used to improve these models in the context of the AIDA project.

Semantic Encoding Tool

As explained above, vector representations, or embeddings, can be efficiently processed by machine learning algorithms and are generally suitable for mathematical operations. *Semantic Encoding* is the process to embed textual data into semantic vector representations that can encode word knowledge and are context aware. These embeddings can be used to solve different downstream NLP tasks such as *Semantic Textual Similarity* presented in the next section.

The aim of the *Semantic Textual Similarity* task is to predict the grade of similarity between two pieces of text from the semantic perspective or, in other words, how similar the meaning of two texts is. A document composed of several paragraphs can incorporate multiple events and topics and provide a grade of similarity between long text is more complex. Generally, the longest the text, the more complex the similarity prediction; for that reason, long text are generally split into sentences or paragraphs and then produced more fine-grained similarity predictions. A community standard dataset used to train semantic textual similarity is the STS-B (*Semantic Textual Similarity Benchmark*) [7] in which sentences and little paragraphs are associated with a similarity score from 0 up to 5 (Table). State-of-the-art models leverage big pretrained language models based on Transformers neural network architecture finetuned on *STS-B* dataset to predict the similarity of a pair of text embeddings through cosine similarity.

5	The two sentences are completely equivalent, as they mean the same thing. <i>The bird is bathing in the sink. Birdie is washing itself in the water basin.</i>
4	The two sentences are mostly equivalent, but some unimportant details differ. Two boys on a couch are playing video games. Two boys are playing a video game.
3	The two sentences are roughly equivalent, but some important information differs/missing. <i>John said he is considered a witness but not a suspect. "He is not a suspect anymore." John said.</i>
2	The two sentences are not equivalent, but share some details. <i>They flew out of the nest in groups. They flew into the nest together.</i>
1	The two sentences are not equivalent, but are on the same topic. <i>The woman is playing the violin. The young lady enjoys listening to the guitar.</i>
0	The two sentences are completely dissimilar. <i>The black dog is running through the snow. A race car driver is driving his car through the mud.</i>

Table – STS-B values overview

In the context of AIDA project, it has been trained a semantic encoder based on the Adapter-Transformers architecture and developed using a python library called Adapter-Transformers⁹. The sentence similarity adapter has been trained using the public STS-B dataset and then fine-tuned on specific project data. Indeed, to fit the trained adapter to the AIDA domain, it has been created a sentence similarity annotation task leveraging specific CC and CT datasets. These datasets have been used to generate sentence pairs related to the project domains, resulting in a new annotated domain specific sentence similarity training dataset.

ANITA innovations in NLP

The ANITA project deals with three main scenarios: 1) Illegal trafficking: drugs, 2) Illegal trafficking: weapons, 3) Terrorism founding. NLP developed in the context of this project has exploited and extended existing taxonomies (see previous section and D3.5) regarding crimes, terrorism and so on, in order to extract a large set of new drugs and weapons and to find the key elements of terrorism founding.

In addition, a very innovative improvement in the field of NLP is represented by the validation flow, through which the analyst/user/LEA of the platform can report to the system if an extracted entity is actually a drug/weapon/precursor. This feedback is then used for further analysis. This allows the ANITA platform to evolve itself and to increase the precision and the recall of the NLP analysis and to learn and update what is useful and what not for the project domain.

The standard extractions are enriched by inferred data to build a complete dataset, as representative as possible to the actual content of the selected sources.

The dataset thus obtained is immediately suitable for the analyses – data aggregations and/or further reasoning operations.

In addition to the standard extractions block, the TAM (Text Analysis Module) produces another block of data, known as New Knowledge, which is managed differently than the first one.

To elucidate what just said, see the text analysis flow step by step.

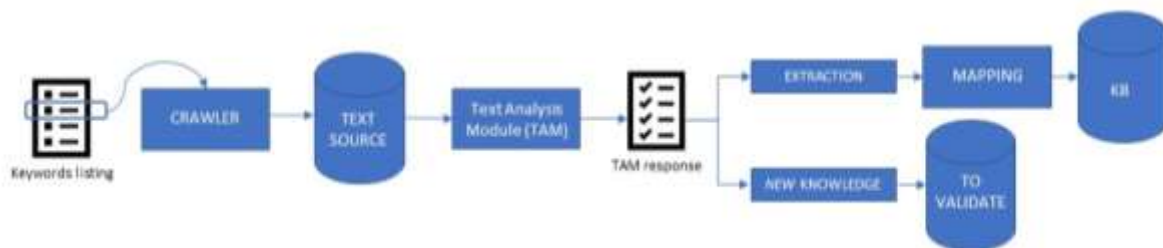


Figure 4: Text Analysis Flow

Crawlers are started by selecting an element from a keyword listing previously defined, texts related to the crawled web sites are obtained and sent to the TAM, which generates a response consisting of two blocks: one containing standard extractions and the other containing new knowledge.

Data of the first block is directly mapped and stored in the knowledge base; this is the extracted data and thus it can be analysed through reasoning operations. Possible inferences are automatically stored in the knowledge base and, together with the pre-existing data, they could be further processed through both reasoning operations and data aggregations.

⁹ <https://github.com/adaptor-hub/adaptor-transformers>

Data of the second block regarding the new knowledge, instead, is not immediately stored because it needs to be validated by domain experts. The extraction of new knowledge is followed by its storage in a dedicated repository; specific web services, New Knowledge Validation, make it possible to read, provide feedbacks and upload valid new knowledge in the knowledge base. Anyway, new knowledge judged not valid is stored in a repository and it is used to avoid proposing already evaluated information whenever extracted again.

Figure 5 shows the validation flow.

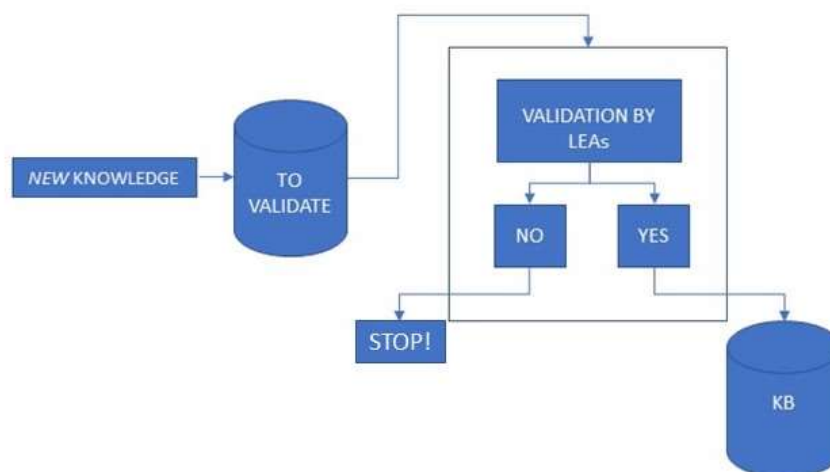


Figure 5: ANITA Validation Flow

Possible scenario

Suppose to monitor the trafficking of ecstasy. It could be helpful to find every substance related to ecstasy itself and also related to its precursors. So, the attention is put on already scheduled substances and on their any other precursors.

All information about known substances defines the prior knowledge of domain and it is extracted from text only if relating to activities of interest. It means it will not be extracted, for example, from scholarly articles in which these substances are scientifically described.

To better explain what said, think to come across a paper like [26]. It reads:

Indeed, the almost perfect solution of blocking two important chemical precursors backfired over time. Instead of importing the prohibited but necessary chemicals, offenders started to produce these chemicals themselves, resulting in the use of pre-precursors (such as safrole for PMK and APAAN for BMK).

In this text, there are some known elements, as safrole, PMK and BMK, and other unknown, as APAAN. Even if PMK and BMK are explicitly present, they are not involved in any activity: they are just mentioned; for this reason, they are not extracted and the resulting TAM response contains only the data available.

NEW KNOWLEDGE	
PRECURSOR	PRECURSOR
Name: <i>safrole</i>	Name: <i>APAAN</i>
Product: <i>PMK</i>	Product: <i>BMK</i>

Figure 6: New Knowledge Extraction

Specifically, the actual new knowledge is:

- Safrole (known substance) as PMK precursor
- APAAN (unknown substance) as BMK precursor

Since safrole and APAAN are detected as *new knowledge*, they are stored in the external repository, labelled as TO VALIDATE to which LEAs have access in order to give feedback on the validity of contained information.

The feedback is provided using the specific validation services and it can be positive or negative. In case of negative feedback, the information thus evaluated is judged NOT VALID and the process stops; otherwise, in case of positive feedback, the information is declared VALID and the respective data is stored in the knowledge base.

Once this data is part of the knowledge base, it enhances reasoning operations. In fact, going back to the example, since safrole is PMK precursor and PMK is ecstasy precursor, it could be inferred that safrole is ecstasy precursor; similarly, for APAAN.

Notice that valid new knowledge enhances generation of inferences and this is its added value, its actual contribution to ANITA.

Additional recommendations

The leaders of the WP5 would like to highlight to the EC a special recommendation emerged while running the research withing this deliverable. It is worth mentioning that almost all the deliverables of the EU funded security projects have dissemination level CO, Consortium Only, and are therefore not publicly readable. Although it is understandable that several results of EC-funded research projects are sensitive – for commercial or strategic reasons – the non-availability of this material to EU researches and practitioners is a great disadvantage as it prevents the exploitation of the research carried out in the past and currently.

This issue arose while contacting the project coordinators to create synergy between the projects, in order to establish clustering and liaison with other ongoing or terminated projects. The NOTIONES project is supposed to collaborate as much as possible with other ongoing related projects to exploit opportunities for knowledge exchange and for improving dissemination among the target audience.

The deliverable leader together with the contributors and the dissemination leader managed to create synergies with several projects in the first year of NOTIONES. It is planned to invite the experts from other projects to participate in open events organized by NOTIONES and take part in the discussion of the active Working Groups. By collaboration in this way, not only we will enlarge the NOTIONES network, but also learn from the success and mistakes from other projects, and perhaps find new focus areas for building new

Working Groups, thus contributing to the EU research in intelligence and security. Nonetheless, there is a concern that the synergy may not be prolific enough assuming that the deliverables of the projects have dissemination level CO.

Consequently, it is highly recommended to consider a request of a creation of new privacy category for the deliverables for the EU funded projects. We do highly recommend making the deliverables public within the topics of the projects, e.g security and intelligence, to be able to exchange the information gathered during the projects with other related projects, thus enhancing the exploitation of the findings.

4.1.2 Technologies and tools

Face Recognition

Facial recognition is a way of identifying or confirming a person's identity by their face. The facial recognition system can be used to identify people in photos, videos or in real time. Facial recognition is a category of biometric authentication systems. Other kinds of biometric authentication systems include voice recognition, fingerprint recognition, and retinal or iris recognition [27]. These technologies are primarily used for security and law enforcement, but there is a growing interest in other areas of use.

Face recognition technology works by matching the faces of people passing by special cameras with images of people on a watchlist. Watchlists can contain photos of anyone, including people who are not suspected of any wrongdoing. Images can come from any source, even social media accounts [28]. There are various facial recognition technologies, but in general they work as follows:

- **Step 1. Face detection.** The camera detects and captures the position of a face image, both alone and in a crowd. The image can be a person looking in front or in profile.
- **Step 2. Face Analysis.** Then a picture is taken and the face image is analyzed. Most facial recognition technologies use 2D rather than 3D images because 2D images are more convenient to match with publicly available photos or photos in a database. The program reads the face geometry. Key factors include the distance between the eyes, the depth of the eye sockets, the distance from the forehead to the chin, the shape of the cheekbones, and the contours of the lips, ears, and chin. The goal is to identify the traits that distinguish this particular person.
- **Step 3: Convert Image to Data.** In the process of analysis, analogue information (face) is converted into a set of digital information (data) based on the facial features of a person. In essence, face analysis is a mathematical formula. The digital code is called a "face print". Each person has their own unique face print, just like fingerprints.
- **Step 4. Search for a match.** The facial print is then compared with data in a database of known faces. For example, the FBI has access to 650 million photographs taken from the databases of various states. On Facebook, all photos tagged with people become part of the Facebook database, which can also be used for facial recognition. If the face print matches the image in the face recognition database, it is determined whose face it is.

Of all biometric identification systems, face recognition is considered the most natural. This is intuitive, since we usually recognize ourselves and others by faces, not by fingerprints and irises. It is estimated that more than half of the world's population regularly encounters facial recognition technologies.

At the state level, facial recognition can help identify terrorists or other criminals, and thus increase security level. On a personal level, facial recognition can be used as a security tool to lock down devices and in personal security cameras. Facial recognition technology is used by law enforcement. According to the NBC

report, the use of this technology is common among law enforcement agencies in the United States and other countries. Police collect photos of detainees and compare them to local, state and federal facial recognition databases. Photos of the detainees are added to databases, which are subsequently used by the police to search for criminals. In addition, mobile face recognition allows police officers to use smartphones, tablets and other handheld devices to take photos of drivers and pedestrians on the spot and immediately compare their photos to facial recognition databases to try to identify them.

Airports and border control. Facial recognition has become commonplace at many airports around the world. More and more travellers have biometric passports. This allows them not to stand in long lines, but to go through automated control of electronic passports and get to the boarding gate faster. Facial recognition not only reduces waiting times, but also improves security at airports. The US Department of Homeland Security predicts that by 2023 facial recognition will be used for 97% of travellers. This technology is used not only at airports and border control, but also to improve security at major events such as the Olympic Games.

Search for the missing. Facial recognition can be used to find missing persons and victims of human trafficking. Suppose the missing people are added to the face recognition database. In this case, law enforcement may be notified as soon as these people are identified by the facial recognition system at an airport, store, or other public place.

Reducing Crime in Retail. Facial recognition is used to identify shoppers who steal goods, retail organized criminals, or people who have been scammed in the past when they enter a store. Photos of people are matched against large databases of criminals, and when shoppers who pose a potential threat enter the store, loss prevention and retail security officers are notified.

Banks. Biometric online banking is another benefit of facial recognition technology. Instead of using one-time passwords, it will be possible to authorize transactions by looking at a smartphone or computer. Thanks to facial recognition technology, attackers will not be able to crack passwords. If attackers steal the database of photographs, "vitality scoring" - the method used to determine whether the source of a biometric sample is a live person or a fake image - should (theoretically) prevent them from using photos from the database to mimic a live person. Thanks to facial recognition technology, debit cards and signatures may become a thing of the past.

Betaface technology

Betaface API is a face detection and face recognition web service. It can scan uploaded image files or image URLs, find faces and analyze them. By comparing images of the faces and faces searches in the database, the API provides verification and identification services, as well able to maintain multiple user-defined recognition databases.

API allows to maintain and perform fast searches in more than 1 million faces collections, arranged in namespaces. In case of necessity to index larger amount of data, additional technical assistance may be provided.

The Betaface API provides the information in the following four categories [29]:

- *"Faces general info:*
 - *multiple faces detection (positions, sizes, angles)*
 - *123 face landmark's locations (22 basic, 101 pro)*
 - *cropped face images*
- Classification:

- *estimate gender, age, ethnicity, emotion (smile/neutral)*
- *detect glasses, moustache, and beard*
- Extended measurements:
 - *face and facial features description (shape, relative size and location)*
 - *eyes, hair, skin, clothes and background colors*
 - *facial hair amount*
 - *approximate hairstyle (length, thickness, form)."*

The software provides an online free demo, which is a great opportunity for the practitioners to test the utility of the application. To sum up Betaface compares single faces or groups of faces and receive similarity confidence along with match decision. When submitting a picture (or an URL) the API will retrieve the face metadata from the image, and use the previously defined metadata tags and stored user-adjusted points and other face info to perform the comparison of single face or even group of faces to receive similarity confidence along to match decision. Also, when downloading a picture, the software will transform the image in order to generate the average from different facial expressions, and modify faces.

4.2 D6.7 recommendations

NOTIONES Work Package 3 “Technologies for Intelligence” studied the state-of-the-art of the technologies useful for Intelligence and Security operations and delivered a rich set of reports for the different types of Intelligence. Following the study of the practitioners’ requirements (WP2), the insights obtained during the first project workshop (T7.1), the discussion among the Working Groups (WP6) and the outcomes of the first project conference (T7.2), both WP3 and WP5 were able to identify the most relevant technologies among those proposed in the reports. Subsequently, it was possible to define some technology priorities, existing gaps and possible roadmaps to fill those gaps, as described in deliverable D6.7 “*Period reporting of findings - v2*”.

It was also possible to indicate and recommend a list of research topics and technologies to be further investigated, namely:

- **AI:** edge AI, AI as a Service (AlaaS), trustworthiness of the AI, updates on the Artificial Intelligence Act (AIA)
- **HUMINT:** explore polygraph lie detection testing by government agencies across EU MSs, P300 brain fingerprinting
- **BIG DATA:** what type of organizational changes are needed in organisations to take the most advantage from it, why LEAs cannot work with commercial actors (cloud, ownership of data, national certification and legacy requirements)
- **IMINT/SIGINT:** sensor/data fusion, improved situational awareness, developments in IMINT and space technologies
- **MASINT:** Wide Area Persistence MASINT CBRNe surveillance from space, X-CUEING concept paradigm
- **MASS SURVEILLANCE:** use of mass surveillance technologies for citizenship manipulation in both online and physical behaviour, privacy-aware surveillance for law enforcement parties

The results of the thematic deepening performed in the second run of WP5 about selected topics in the list above are presented as Annexes to this deliverable:

- Annex I – EU framework on Artificial Intelligence, by Z&P
- Annex II – The relationship between LEAs and commercial actors, by DRI
- Annex III – Trustworthiness of the AI, by KhNUIA
- Annex IV – Artificial Intelligence as a Service, by KhNUIA
- Annex V – P300 technology for HUMINT, by Z&P and SAHER

5. 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.

INSPECTr project

The NOTIONES practitioners have expressed interest in technological solutions aimed at enhancing the secure data sharing and dissemination. The EU-funded INSPECTr project seems to be a highly relevant initiative because it aims at developing a shared intelligence platform that will improve digital and forensic capabilities, and reduce the complexity and cost of cross-border collaboration.

FOCUS AREA: Secure Data Sharing and Dissemination
KEYWORD / TYPE: platform, Data Sharing, Evidence correlation and transfer

INSPECTr

DESCRIPTION:
 Cybercrime is a borderless crime that leverages technology and the internet to exploit businesses, communities and individuals. Law enforcement officers responsible for investigating cybercrime need to be equally able to access cutting edge technology to combat these crimes and to bring down criminal networks. The EU-funded INSPECTr project will integrate a range of high-tech approaches, including Big Data analytics, cognitive machine learning and blockchain technologies into a shared intelligence platform that will improve digital and forensic capabilities, and reduce the complexity and cost of cross-border collaboration. The platform will incorporate privacy and ethics by design principles, and will take into account relevant national and international legislation.

PROJECT: INSPECTr (Intelligence Network and Secure Platform for Evidence Correlation and Transfer)

TYPE OF PROJECT: RIA SU-FCT02-2018-2019-2020

YEAR: 2019-2023

PoC: UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN (Ireland)

SOURCE OF INFORMATION: <https://inspectr-project.eu/>, <https://cordis.europa.eu/project/id/833276>

COMMENTS: INSPECTr adopted a common format for data homogenisation, linked cases and data exchange: the open-source Cyber-investigation Analysis Standard Expression (CASE, <https://caseontology.org>) language, a community-developed ontology designed to serve as a standard for interchange, interoperability, and analysis of investigative information in a broad range of cyber-investigation domains, including digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence, and situational awareness.

T5.2 – M13

Figure 7 - Main results: INSPECTr project

i-LEAD results

i-LEAD represents a similar project with respect to NOTIONES: they both aim at building a pan-European network of practitioners that can express requirements and priorities on innovative technologies. I-LEAD is dedicated to Law Enforcement practitioners, while NOTIONES is dedicated to Intelligence and Security practitioners. It is not clear whether these two categories share the same perspective.

i-LEAD started in 2017 and is now approaching its conclusion - it will end in 2023 – and in the past years it has delivered many reports and documents stating the perspective of law Enforcement on digital investigations, crime scene recording and documentation, vehicle mitigation, crime as a service and others.

NOTIONES practitioners should carefully read these documents and provide feedback on the recommendations on standardisation and procurement provided there, highlighting existing convergences or divergences of opinions, needs and expectations and delivering specific recommendations from the perspective of Security and Intelligence practitioners.



Figure 8 - Main results: i-LEAD project

LAW-GAME

The overarching objective of LAW-GAME is to train police officers on the procedure, enhancing the transition between the theory and real-life practice through gamification technologies in a safe and controlled virtual environment.

To achieve this, the project introduces an attractive approach for assisting the development of core competencies required to perform intelligence analysis through a series of AI-assisted procedures for crime analysis and the prediction of illegal acts, all within the LAW-GAME game realm.

FOCUS AREA: Training

KEYWORD / TYPE: platform, games, LEAs

LAW-GAME

DESCRIPTION:

LAW-GAME project will use gamification technologies to train police officers, introducing an attractive method to develop competencies required to perform AI-assisted intelligence analysis and illegal acts prediction. LAW-GAME will conduct forensic examination through a one-player or multi-player cooperative scenario and provide developed AI tools for evidence recognition, crime scene investigation, and car accident analysis. The project will expose the trainees to police interview tactics and train them to recognise and mitigate potential terrorist attacks. Building upon an in-depth analysis of police officers' learning needs, LAW-GAME will develop an advanced learning experience, embedded into 3 comprehensive "gaming modes" dedicated to train police officers and measure their proficiency in: 1) conducting forensic examination, 2) effective questioning, threatening, cajoling, persuasion, or negotiation, 3) recognizing and mitigating potential terrorist attacks.

PROJECT: LAW-GAME (An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions)

TYPE OF PROJECT: RIA H2020-SU-SEC-2018-2019-2020

YEAR: 2021-2024

PoC: TECNALIA (Coordinator of NOTIONES) is in the Consortium of LAW-GAME

SOURCE OF INFORMATION: <https://lawgame-project.eu/>, <https://cordis.europa.eu/project/id/101021714>

COMMENTS: The project is ongoing and appears to be very interesting for NOTIONES with respect to the focus area "Improvements and Innovations to Various Intelligence Related Training".

T5.2 – M13

Figure 9 - Main results: LAW-GAME project

The project is ongoing and appears to be very interesting for NOTIONES with respect to the focus area "Improvements and Innovations to Various Intelligence Related Training".

Cyber Ranges

Cyber Ranges are the new frontier of CyberSecurity preparedness and training. There are several EU initiatives and research projects about cyber ranges, federated cyber ranges, cyber ranges built with commercial solutions, software-only cyber ranges and others.

FOCUS AREA: Cybersecurity, training
KEYWORD / TYPE: software, IT environment

Cyber Ranges

DESCRIPTION:
 Cyber ranges are platforms for the development, delivery and use of interactive simulation environments representing organisation's ICT, OT, mobile and physical systems, applications and infrastructures. The cyber ranges allow the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon.
 Cyber ranges can be federated into a larger cluster with more capacity and unique services.

STATUS: the technology is already at TRL 9 for certain applications and many EU-funded research projects are developing it in different fields

EXPECTED OPERATIONAL USE: simulation of real-world cyber attacks for prevention and training

POSSIBLE BENEFITS: Federated Cyber Ranges software-only solutions can perform with high throughput, low latency and low CPU usage

DISCUSSION TOPICS: Commercial solutions have proven to be suitable to build Federated Cyber Ranges, although skilled workforce to plan and implement a federation network is required. The NOTIONES network may discuss if this sort of solutions meet the requirements of the practitioners.

RELATED EU-FUNDED PROJECTS: ECHO, CYCLOPES, CyberSec4Europe

T5.3, T5.2 – M13

Figure 10 - Main results: cyber ranges

NOTIONES should investigate if practitioners are interested in cyber ranges, what are their expectations and requirements on them, to what extent they need them for training purposes and for which applications.

P300 technology

Deliverable D6.7, receiving the recommendations from WP3, reported the need to examine and explore the potential of P300-related cognitive technologies for deception detection by government agencies across EU Member States and identify the potential positive applications and operational challenges and considerations for HUMINT and other intelligence disciplines following analysis of the use by police authorities in the UAE.

WP5 investigated this topic and interesting information was found.

FOCUS AREA: HUMINT
KEYWORD / TYPE: brain fingerprinting

P300 technology

DESCRIPTION:
 Brain fingerprinting is a controversial investigative technique that measures whether specific information is stored in a subject's brain. The technique consists of measuring, through electroencephalography (EEG), a person's electrical brainwave response to words, phrases, or pictures that are presented on a computer screen. Brain fingerprinting was invented by Lawrence Farwell in the 1990s. Its theory explains that the suspect's reaction to the details of an event or activity will reflect if the suspect had prior knowledge of the event or activity. Farwell's brain fingerprinting originally used the well-known P300 brain response to detect the brain's recognition of the known information, thus the name "P300 technology".

STATUS: application of Brain Fingerprinting testing in criminal case has been successfully tested

EXPECTED OPERATIONAL USE: to determine scientifically whether or not specific information is stored in the suspect's brain

POSSIBLE BENEFITS: Brain fingerprinting testing provides an accurate, economical, and timely solution to the problem of the fight against terrorism. This technique can determine with an extremely high degree of accuracy those who are involved in terrorist activity and those who are not.

DISCUSSION TOPICS: to scope the potential operational opportunities, applications and impacts upon intelligence operations and law enforcement investigations.

T5.3 – M13

Figure 11 - Main results: P300 technology

It is recommended that brain-fingerprinting and related P300 tools, tactics, techniques and technologies be subject to further monitoring and analysis conducted with end-user practitioners to scope the potential operational opportunities, applications and impacts upon intelligence operations and law enforcement investigations. This scoping activity will inform a roadmap of research requirements proving an evidence base to support for future security research programming.

6. Conclusions and next steps

This document represents the product of the second run of tasks T5.2 and T5.3 of WP5, which performed the research monitoring activities during months M13 and M14 (September, October 2022).

Task T5.2 performed the horizon scanning activity through exploratory research on the online scholar database The Lens, the CORDIS database and the open web. Results were found about Digital forensics methods and initiatives, EU-level training for Law Enforcement, technologies for fighting Cybercrime and enhancing Cyber Security (especially Cyber Ranges), and EU-projects relevant in these areas.

Task T5.3 performed the monitoring of EU-funded research projects on the CORDIS database and found 29 new projects with topic related to the focus areas: “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”, “Technological Solutions to Secure Data Sharing and Dissemination (internally and externally)”, “cybersecurity and cybercrime”, “Artificial Intelligence” and other technological innovation areas - including platforms, CBRNE tools, and training for LEAs.

WP5 also took care of the research projects and technologies/tools that gained more votes in the Working Groups organized by task T6.1, which deserved further deepening and possibly interaction. On one hand, in regard of the research projects, it was possible to contact and start interaction with projects AIDA, ALIGNER, ANITA, CTC, ECHO, INFINITY, PopAI, PREVISION and INSPECTr. Extended information on the innovation potential of projects ANITA and AIDA was obtained. On the other hand, little information was found about the technologies and tools voted by the practitioners, apart from what is already available online in the technology providers’ websites. Technology providers may be more prone to answer contact requests made directly by practitioners. It is also possible that they use other channels to find potential customers, such as trade shows and specialized events, instead of direct contact. This is a big issue that must be carefully discussed in NOTIONES, so that a good strategy can be planned towards the risk of not being able to reach technology providers.

Finally, WP5 performed thematic deepening on selected topics indicated by task T6.7 as recommended for further investigation. The reports are presented as Annexes to this deliverable and regard: the EU framework on Artificial Intelligence, the relationship between LEAs and commercial actors, the trustworthiness of the AI, the Artificial Intelligence as a Service, and the P300 technology.

In conclusion, the results of the second run of tasks T5.2 and T5.3 were documented in this report. The main findings are summarised in section 5, highlighting technologies and EU projects that are most promising for the purposes of NOTIONES:

- INSPECTr project;
- I-LEAD project;
- LAW-GAME project;
- Cyber ranges;
- P300 technology.

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 M19-M20:

- 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 with updated search parameters;
- 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 D5.4 “*Monitoring of EU Research and Horizon Scanning -v3*”, due in M20.

References

- [1] TheLens. [Online]. Available: <https://www.lens.org/>.
- [2] Publications Office of the European Union, “COMmunity Research and Development Information Service,” [Online]. Available: <https://cordis.europa.eu/en>.
- [3] G. Gulati, A. Cusack, V. Murphy, B. D. Kelly, S. Kilcommins and C. P. Dunne, “The evaluation of a training course to enhance intellectual disability awareness amongst law enforcement officers: a pilot study,” *Irish journal of psychological medicine*, pp. 1-5, 2021.
- [4] G. Gulati, B. D. Kelly, A. Cusack, S. Kilcommins and C. P. Dunne, “The experience of law enforcement officers interfacing with suspects who have an intellectual disability – A systematic review,” *International journal of law and psychiatry*, vol. 72, p. 101614, 2020.
- [5] K. Lorey and J. M. Fegert, “Increasing Mental Health Literacy in Law Enforcement to Improve Best Practices in Policing-Introduction of an Empirically Derived, Modular, Differentiated, and End-User Driven Training Design,” *Frontiers in psychiatry*, p. 706587, 2021.
- [6] K. Lorey and J. M. Fegert, “Incorporating mental health literacy and trauma-informed law enforcement: A participative survey on police officers' attitudes and knowledge concerning mental disorders, traumatization, and trauma sensitivity,” *Psychological trauma : theory, research, practice and policy*, vol. 14, no. 2, pp. 218-228, 2021.
- [7] M. T. Compton, S. B. B. Krishan, R. Bakeman, M. H. Fleischmann, D. Hankerson-Dyson, L. Husbands, T. Stewart, B. D'Orion, B. del Pozo and A. C. Watson, “Using the Theory of Planned Behavior to Understand How Crisis Intervention Team (CIT) Training Facilitates Police Officers' Mental Health Referrals,” *Community mental health journal*, vol. 58, no. 6, pp. 1-9, 2021.
- [8] R. Ferguson, R. Karen, S. Wilford and A. Irons, “PRECEPT: a framework for ethical digital forensics investigations,” *Journal of Intellectual Capital*, vol. 21, no. 2, pp. 257-290, 2020.
- [9] P. H. Hartel and R. van Wegberg, “Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases.,” *arXiv: Cryptography and Security*, 2021.
- [10] G. Humphries, R. Nordvik, H. Manifavas, P. Copley and M. Sorell, “Law enforcement educational challenges for mobile forensics,” *Forensic Science International: Digital Investigation*, vol. 8, no. DFRWS 2021 APAC - Proceedings of the First Annual DFRWS APAC, p. 301129, 2021.
- [11] A. o. C. P. Officers, “ACPO good practice guide for digital evidence,” 2012.
- [12] ISO, “17025,” 2017.
- [13] E. N. o. F. S. Institutes, “Best practice manual for the forensic examination of digital technology,” 2015.
- [14] S. W. G. o. D. Evidence, “SWGDE best practices for mobile device evidence collection & preservation, handling, and acquisition,” 2019.

- [15] D. Schröder, G. Bóta and M. Molina Sierra, “Combatting illicit tobacco trade: What is the role of EU law enforcement training?,” *Tobacco prevention & cessation*, vol. 7, no. March, pp. 18-18, 2021.
- [16] CEPOL, “European Union Agency for Law Enforcement Training,” [Online]. Available: <https://www.cepola.europa.eu/>. [Accessed 30 9 2022].
- [17] EUROPOL, “EMPACT 2022+ Fighting crime together,” [Online]. Available: <https://www.europol.europa.eu/crime-areas-and-statistics/empact>. [Accessed 30 9 2022].
- [18] S. Baadel, F. Thabtah and J. Lu, “Cybersecurity Awareness: A Critical Analysis of Education and Law Enforcement Methods,” *Informatica*, vol. 45, no. 3, p. 335–345, 2021.
- [19] E. Commission, “Cybercrime,” [Online]. Available: https://home-affairs.ec.europa.eu/cybercrime_en. [Accessed 30 9 2022].
- [20] Europol, “EC3,” [Online]. Available: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>. [Accessed 30 9 2022].
- [21] A. Grigoriadis, E. Darra, D. Kavallieros, E. Chaskos, N. Kolokotronis and X. Bellekens, “Cyber Ranges: The New Training Era in the Cybersecurity and Digital Forensics World,” *Security Informatics and Law Enforcement*, pp. 97-117, 2021.
- [22] ECSO, “Understanding Cyber Ranges: From Hype to Reality,” 2020.
- [23] CyberSec4Europe, “Cyber Range Federation – The Real Benefits,” 29 10 2021. [Online]. Available: <https://cybersec4europe.eu/cyber-range-federation-the-real-benefits/>. [Accessed 10 10 2022].
- [24] A. Grigoriadis, E. Darra, D. Kavallieros, E. Chaskos, N. Kolokotronis and X. Bellekens, “World, Cyber Ranges: The New Training Era in the Cybersecurity and Digital Forensics,” in *Technology development for Security practitioners*, Springer, 2021, pp. 97-117.
- [25] H. S. J.-S. S. F. M. & J.-L. G. Yoshua Bengio, *Neural Probabilistic Language Models*, Springer, 2006.
- [26] E. Kleemans and M. Soudijn, “Organised crime,” in *Handbook of Crime Prevention and Community Safet*, Routledge, 2017.
- [27] J. Lynch, “ Face Off: Law Enforcement Use of Face Recognition Technology,” *Electronic Frontier Foundation*, 2020.
- [28] X. M. LIXIANG LI, “A Review of Face Recognition Technology,” *IEEE Access*, vol. 8, 2020.
- [29] “Betaface,” [Online]. Available: <https://www.betafaceapi.com/> .
- [30] D. A. a. B. Singh, “Brain fingerprinting,” *Journal of Engineering and Technology Research*, vol. 4, no. 6, pp. 98-103, 2012.

Annex I EU framework on Artificial Intelligence

Artificial intelligence is a family of technologies that display intelligent behaviour by analysing their environment and taking actions, with some degree of autonomy, to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world – i.e., voice assistants, search engines, or face recognition systems – or AI can be embedded in hardware devices – i.e., advanced robots, autonomous cars, or drones. Many AI technologies require data to improve their performance. Once they perform well, they can help improve and automate decision-making in the same domain. For instance, an AI system can be trained and then used to spot cyber-attacks based on data from the concerned network or system [1]. In general, AI can optimise existing processes or enable brand-new activities, offering new opportunities and benefits for business and public services, but also serious risks. As first observed by the European Parliament in the Resolution of 16 February 2017 on Civil Law Rules on Robotics, the use of systems regulated by AI involves risks that are different from those linked to the human factor, inevitably posing ethical and legal problems [2]. With regards to privacy, it can be endangered by the unregulated use of facial recognition in public spaces. Furthermore, based on the design and type of data entered, AI systems could reproduce the existing discrimination in the offline world, making decisions influenced by ethnicity, gender, or age class. Nowadays, the AI has its responsibilities for the so-called “filter bubbles” – the virtual environments that each user builds on the Internet through his preferential selections, characterized by low permeability to novelty and a high level of self-referentiality due to the always similar contents proposed by the algorithm. The so-called “deepfakes” – false but extremely realistic visual and audio contents, which are increasingly used in the field of information warfare – are also created through AI.

Still, the benefits brought by artificial intelligence are enormous. Faced with the rapid technological development determined by the growth of solutions based on artificial intelligence – the number of patent applications published in the last decade has increased by + 400% – and with an international context in which the main competitors of the European Union are heavily investing in this technology, the European Commission has adopted a series of initiatives aimed at regulating AI. By optimizing operations and resource allocation, according to EP estimates, the use of AI will lead to an increase in labour productivity between 11 and 37% by 2035 [3]. From predictive maintenance to collaborative robots, from digital twins to augmented reality, AI applications will improve machinery maintenance and extend production processes in terms of quality and quantity. The new generation of products and services related to AI could generate a reduction of global greenhouse gas emissions between 1.5% and 4% by 2030 [3].

However, fragmentation of national actions with regard to AI applications as a risk to EU global competitiveness and standard setting was the main reason that prompted the EC to launch the European Strategy on Artificial Intelligence in April 2018 [4]. The main assumption at the basis of the European strategy is that the EU “can lead the way in developing and using AI for good and for all, building on its values and its strengths”. These strengths include the following: world-class researchers, labs, and start-ups; the Digital Single Market; a wealth of industrial, research and public sector data which can be unlocked to feed AI systems [1]. Within its strategy, the European Commission then identified three distinct but complementary commitments: (a) increase investments to a level that corresponds to the economic weight of the European Union in the world; (b) leave no one behind – especially in the education field – and ensure a smooth transition to the era of artificial intelligence in the workplace; (c) ensure that new technologies reflect European values and principles. With respect to this last commitment, the EC made explicit reference to the General Data Protection Regulation (GDPR) of 2016 on data protection and privacy in the European space – which at the time was not yet in force [5] – and to Article 2 of the Treaty on European Union (TEU), which lists the founding values of the European political community: “respect for human dignity, freedom,

democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities” [6].

In the aforementioned Communication, the European Commission also announced the adoption of a series of initiatives on artificial intelligence, including the launch of the European AI Alliance, which is a multi-stakeholder forum that has rapidly attracted members of civil society, industry and the academic world, and the institution of a High-Level Expert Group on Artificial Intelligence (AI HLEG) [7]. The 52 experts of the AI HLEG were asked by the EC to develop a set of ethical guidelines, published in April 2019 under the name of Ethics Guidelines for Trustworthy AI [8], and to make policy and investment recommendations, which were presented in June 2019 in the document Policy and Investment Recommendations for Trustworthy AI [9]. Overall, these two documents highlighted the need to join forces at a European level, in order to develop a human-centred approach to artificial intelligence as the main feature of “AI made in Europe”. This vision was reaffirmed by the EC itself in COM (2019)168 entitled “Building Trust in Human-Centric Artificial Intelligence” of April 2019 [10]. Finally, on July 2020 the AI HLEG presented its final Assessment List for Trustworthy Artificial Intelligence (ALTAI), identifying seven key requirements – human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; environmental and societal well-being; accountability – to ensure that users benefit from AI without being exposed to unnecessary risks by indicating a set of concrete steps for self-assessment [11].

The European Strategy on Artificial Intelligence was followed by the White Paper on Artificial Intelligence of February 2020, accompanied by a Communication from the EC itself outlining the European Strategy for Data [12] [13]. In general, the document suggested establishing within the European space both an “ecosystem of excellence” in the development and diffusion of AI systems, and an “ecosystem of trust” based mainly on a human-centric approach to artificial intelligence. The White Paper was also accompanied by the “Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics”, concluding that the current product safety legislation contains a number of gaps that needed to be addressed, notably in the Directive 2006/42/EC – the so-called “Machinery Directive” [14] [15].

During the development of the EU framework on artificial intelligence, the European institutions have also given importance to the security aspect of AI systems. In December 2020, the European Union Agency for Cybersecurity (ENISA) presented a report called “Artificial Intelligence Cybersecurity Challenges”, warning that AI may open new avenues in manipulation and cyber-attack methods, as well as new privacy and data protection challenges for citizens, enterprises, and institutions [16]. The main highlights of the report include the following: definition of the scope of AI in the context of cybersecurity following a lifecycle approach, from requirements analysis to deployment; identification of assets of the AI ecosystem as a fundamental step in pinpointing what needs to be protected and what could possibly go wrong in terms of security of the AI ecosystem; mapping of the AI threat landscape by means of a detailed taxonomy; classification of threats for the different assets and in the context of the different AI lifecycle stages, also listing relevant threat actors; analysis of the impact of threats to different security properties [16]. In recent years, the EU defence sector has become interested in AI too. It is reported the workshop hosted in June 2021 by the European Defence Agency (EDA) called “Defence Applications of Artificial Intelligence” (DAAI 2021), which was part of the International Conference on Artificial Intelligence Applications and Innovations (AIAI 2021) [17].

In defining its approach to AI, the European Union has decided to play the role of pioneer in the sector, similar to what it did with the GDPR of 2016. With COM (2021)205 of 21 April 2021, the EC has in fact announced an ambitious regulatory project on AI, which is still under development [18]. On the same date, the European Commission proposed to the European Parliament and the Council of the EU a regulation on harmonised rules regarding AI applications – the so-called “Artificial Intelligence Act” – emphasising that its approach is shaped by European values and risk-based, ensuring both safety and fundamental rights protection [19].

Once approved, this regulation would represent the first legal framework in the world on the AI sector. As stated in the proposal: “By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society” [19]. The EU has therefore decided to regulate these elements and lay the necessary legal bases so that artificial intelligence has rules and specific guidelines within the common European space.

The appropriate balance between fundamental rights protection and public security is indeed one of the main pillars of the proposal. The European Union wants to ensure that European citizens can benefit from safe, transparent, ethical, and impartial AI systems under human control, thus placing specific requirements for all European or foreign AI systems used in the EU territory. Specifically, it aims at addressing risks of specific uses of AI, categorising them into 4 different levels: “unacceptable risk”, “high risk”, “limited risk”, and “minimal risk”. In doing so, the AI regulation will make sure that Europeans can trust the artificial intelligence they are using. For instance, the “unacceptable risk” category includes AI applications in which algorithms track users’ behaviour to automatically assess what level of creditworthiness to grant to individuals and companies – they are widely used in China. Examples of elements classified as “high risk” are the following: AI systems that autonomously control critical infrastructures; AI applications that could endanger the life and health of citizens; CV sorting software for hiring procedures. All these systems will be carefully evaluated before being placed on the market, will be subject to minimum transparency obligations and will be monitored throughout their life cycle. Anyway, the vast majority of artificial intelligence systems fall into the category of “minimal risk”, therefore they will not be subject to the new European legislation.

Particular attention must be paid to biometric surveillance. Artificial intelligence powers the use of biometric technologies, including facial recognition applications, which are used for verification, identification, and categorisation purposes by private or public actors. While facial recognition markets are poised to grow substantially in the coming years, the increasing use of facial recognition technologies (FRTs) has emerged as a salient issue in the worldwide public debate on biometric surveillance. While there are real benefits in using facial recognition systems for public safety and security, their pervasiveness and intrusiveness, as well as their susceptibility to error, give rise to a number of fundamental rights concerns with regard, for instance, to discrimination against certain segments of the population and violations of the right to data protection and privacy [20]. In October 2021, the European Parliament passed a non-binding resolution that prevents the use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement, along with the creation of private facial recognition databases. With this resolution, the EP recognized that the use of AI for mass surveillance and other unlawful interference, such as the profiling of citizens in order to rank them and restrict their freedom of movement, pose a serious threat to fundamental rights [21]. The non-binding resolution sends a strong signal on how the EP is likely to vote in upcoming negotiations on the Artificial Intelligence Act.

The legislative framework on artificial intelligence will have a huge impact worldwide, as it was for the GDPR of 2016, which has become an international standard in its sector since it came into effect in 2018. With this proposal, the EU wanted to strengthen its competitive position with respect to its main competitors – China and the United States of America – by anticipating them in the definition of a regulatory framework that could thus become the reference standard on the global scene. This political dimension was reaffirmed by the Coordinated Plan on Artificial Intelligence 2021 Review, which goes hand in hand with the proposal for the Artificial Intelligence Act [22]. The new plan builds on the collaboration established between the EC and

Member States – plus Norway and Switzerland – during the 2018 Coordinated Plan on Artificial Intelligence, which was a joint commitment to maximising Europe’s potential to compete globally and an essential first step in defining actions and funding instruments for the uptake and development of AI across sectors. Moreover, it encouraged Member States to develop national strategies [23] [24]. The revised plan proposes around 70 actions for closer and more efficient cooperation between the EC and Member States on artificial intelligence between 2021 and 2027.

As already outlined in the White Paper on Artificial Intelligence of February 2020, the European Commission has thought about a series of tools to support the future legislation, in order to favour the birth of a public-private partnership on artificial intelligence, data and robotics to define, implement and invest in a joint strategic research and innovation program for Europe. These tools include the establishment of centres of excellence for AI, the birth of new digital innovation poles that act as one-stop shops to provide access to technical skills and experimentation – so that companies can “test before investing” – and the creation of a central European database of AI resources needed for the uses of private companies and the public sector. With funds provided by the Digital Europe (DIGITAL) and Horizon Europe (HE) programs, the European Commission intends to invest around one billion euros per year in AI and mobilize further investment from the private sector and Member States through their National Recovery and Resilience Plans (NRRPs) for a total of 20 billion a year [25].

Schematically, the European approach to artificial intelligence has four fundamental objectives: (a) establish the enabling conditions for the development and diffusion of AI; (b) build a strategic leadership in high impact sectors; (c) making the EU a place where AI can flourish; (d) ensure that AI technologies serve people. These objectives fall within the broader concept of a continent that sees in technological progress, attentive to the environment and human society, not only one of the keys necessary for the post-pandemic restart, but above all an indispensable tool for an ever-greater integration between Member States in a single entity capable of relating equally to the great world powers.

In recent years, the main competitors of the EU have recognized the revolutionary nature of AI and have adopted different approaches to artificial intelligence that reflect their political, economic, cultural and social systems [26]. On one hand, the National AI Initiative Act of 2020 became law in January 2021 and provides for a coordinated program across the entire Federal government of the United States to accelerate AI research and application for the American economic prosperity and national security. Its primary mission is to ensure continued US leadership in AI research and development, lead the world in the development and use of trustworthy AI in the public and private sectors, and prepare the present and future American workforce for the integration of AI systems across all sectors of the economy and society [27]. On the other hand, the 2017 China’s government released the New Generation AI Development Plan for 2030 aims at surpassing its rivals technologically and setting a goal of becoming a global innovation centre in this field by that date [28]. Other countries such as the UK, Japan and Canada have also adopted national AI strategies [29] [30] [31]. From a political point of view, the intention of Brussels is to trace a “third way” between the extremely free market of the United States of America – where cases such as the Clearview AI platform have already generated several legal battles [32] – and the authoritarianism of China – where mass surveillance through facial recognition is already a reality and where the Social Credit System, which tracks every aspect of a citizen’s life and determines the services that can be use, is in an advanced state of experimentation [33].

However, the delay of the European Union in terms of technological development in certain sectors risks putting it at a disadvantage in the current political landscape. On March 2022, the European Parliament’s Special Committee on Artificial Intelligence in a Digital Age (AIDA) adopted a report on artificial intelligence. On one hand, it emphasised that the digital transition in the EU must be human-centric and compatible with the Charter of Fundamental Rights of the European Union. On the other hand, the report cautioned that the

EU has fallen behind in the global race for technological leadership. This might result in a risk for standards that need to be developed elsewhere in the future, often by non-democratic actors [34]. The delay of the EU compared to its main competitors is the reason why the European Commission proposed the creation of the EU-US Trade and Technology Council (TTC), which was established in June 2021 to promote coordination between the two shores of the Atlantic Ocean on everything related to the technology sector – from regulation to taxation, passing through cybersecurity [35]. On May 2022, meeting at the second Ministerial Summit of the TTC in Paris, both parties discussed the implementation of common AI principles and agreed to develop a joint roadmap on evaluation and measurement tools for trustworthy AI and risk management [36]. However, the European approach places the European Union at the forefront of regulation in the field of artificial intelligence, as happened with the GDPR of 2016. In the end, given the European focus on the values underlying the rules, aimed at avoiding the systematic violation of privacy and individual freedoms as happens in the Chinese system, it seems that the EU and the US are destined to converge in this sector. From a long-term perspective, it is crucial that the EU – in the search for strategic autonomy – continues to allocate public resources for the development of an “AI made in Europe” and favours the creation of a European environment that stimulates private investment.

The legislative process relating to the proposed regulation is currently proceeding. The EP Committee on the Internal Market and Consumer Protection (IMCO) and the EP Committee on Civil Liberties, Justice and Home Affairs (LIBE) jointly released a draft report on the EC proposal in April 2022. The document includes proposed amendments to the original text proposed by the European Commission. The most significant changes proposed in the draft report include the ban on using artificial intelligence to implement predictive policing practices, the obligation to register AI-based technologies and greater alignment with the GDPR [37].

Regarding the timing of the approval of the Artificial Intelligence Act, it is possible to make a parallel with the General Data Protection Regulation by virtue of their ambition to become an international standard. Conceiving the EC proposal of January 2012 for a comprehensive reform of Directive 95/46/EC – the so-called Data Protection Directive [38] – as the first step of the legislative process, then it took about 4 years to reach the approval of the GDPR, which occurred in April 2016. This takes into account that the aforementioned regulation has been effective in all Member States of the European Union only since May 2018 [5]. The European Commission unveiled the proposal for an EU regulatory framework on artificial intelligence in April 2021. Considering the comparison between the two legislative frameworks valid, it is reasonable to expect the approval of the Artificial Intelligence Act for 2025. However, there are many factors that can intervene to speed up the approval process. First, in recent years the European Union has recognized the importance of achieving greater strategic autonomy, especially in the technological field. Moreover, the current international context is more competitive than in the previous decade, therefore it requires greater speed and cohesion in the adoption of legislative measures aimed at safeguarding the European interests. Finally, other European institutions and the main Member States have shown full support towards the EC proposal, suggesting there will be no great opposition to the presented text. Given the overmentioned situation, it is possible that a definition of the EU framework could be reached far in advance, even in 2023. By the end of 2022, final amendments are expected to be adopted by the European Parliament during plenary session; then, the outcome will be discussed by the Council of the EU. Subsequently, as established by the procedure, a trilogue will be launched between representative of the European Commission, the European Parliament and the EU Council to arrive at the definition of an agreed text. According to journalistic sources, this will take place in the spring of 2023, while it will take further months for its effective implementation – in other terms, to ensure that the target market can absorb the new regulation and react accordingly [39]. Once the Regulation is approved, it will be necessary to draw up guidelines to facilitate its implementation, since it is essential to harmonize the Artificial Intelligence Act with the other EU sectoral regulatory instruments. It is clearly a massive task, which will require a great deal of effort from the entire EU system and the Member

States, in order to make the AI tool and the regulatory framework transparent, effective and suitable for a constantly evolving market.

References

- [1] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe,” 25 April 2018. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&rid=1>. [Accessed 31 May 2022].
- [2] European Parliament, “European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics,” 16 February 2017. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&from=EN>. [Accessed 31 May 2022].
- [3] European Parliament, “Artificial intelligence: Threats and Opportunities,” 4 May 2022. [Online]. Available: https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200918STO87404/20200918STO87404_en.pdf. [Accessed 3 June 2022].
- [4] European Parliamentary Research Service (EPRS), “European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies,” 28 September 2020. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU\(2020\)654179_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf). [Accessed 3 June 2022].
- [5] European Parliament and Council of the EU, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and [...], and Repealing Directive 95/46/EC (General Data Protection Regulation),” 27 April 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. [Accessed 31 May 2022].
- [6] Official Journal of the European Union, “Consolidated Version of the Treaty on European Union - Title I Common Provisions - Article 2,” Official Journal of the European Union, 26 October 2012. [Online]. Available: https://eur-lex.europa.eu/eli/treaty/teu_2012/art_2/oj. [Accessed 3 June 2022].
- [7] European Commission, “The European AI Alliance,” European Commission, [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>. [Accessed 3 June 2022].
- [8] European Commission, “Ethics Guidelines for Trustworthy AI,” European Commission, 8 April 2019. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. [Accessed 3 June 2022].
- [9] High-Level Expert Group on Artificial Intelligence (IA HLEG), “Policy and Investment Recommendations for Trustworthy AI,” 26 June 2018. [Online]. Available: https://www.europarl.europa.eu/italy/resource/static/files/import/intelligenza_artificiale_30_aprile/ai-hleg_policy-and-investment-recommendations.pdf. [Accessed 3 June 2022].
- [10] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building Trust in Human-Centric Artificial Intelligence,” European Commission, 8 April 2019. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence>. [Accessed 3 June 2022].
- [11] European Commission, “Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment,” European Commission, 17 July 2020. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>. [Accessed 3 June 2022].
- [12] European Commission, “White Paper on Artificial Intelligence - A European Approach to Excellence and Trust,” 19 February 2020. [Online]. Available: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. [Accessed 31 May 2022].
- [13] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European Strategy for Data,” 19 February 2020. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>. [Accessed 4 June 2022].

- [14] European Commission, “Commission Report on Safety and Liability Implications of AI, the Internet of Things and Robotics,” European Commission, 19 February 2020. [Online]. Available: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en. [Accessed 4 June 2022].
- [15] European Parliament and Council of the EU, “Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on Machinery, and amending Directive 95/16/EC (Recast),” 9 June 2020. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=EN>. [Accessed 4 June 2022].
- [16] European Union Agency for Cybersecurity (ENISA), “Artificial Intelligence Cybersecurity Challenges,” European Union Agency for Cybersecurity (ENISA), 15 December 2020. [Online]. Available: <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>. [Accessed 3 June 2022].
- [17] European Defence Agency (EDA), “EDA Pursues Work on Artificial Intelligence in Defence,” European Defence Agency (EDA), 29 June 2021. [Online]. Available: <https://eda.europa.eu/news-and-events/news/2021/06/29/eda-pursues-work-on-artificial-intelligence-in-defence>. [Accessed 4 June 2022].
- [18] European Commission, “Communication on Fostering a European Approach to Artificial Intelligence,” European Commission, 21 April 2021. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence>. [Accessed 4 June 2022].
- [19] European Commission, “Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts,” 21 April 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. [Accessed 31 May 2022].
- [20] European Parliamentary Research Service (EPRS), “Regulating Facial Recognition in the EU,” September 2021. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf). [Accessed 4 June 2022].
- [21] European Parliament, “Use of Artificial Intelligence by the Police: MEPs Oppose Mass Surveillance,” European Parliament, 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>. [Accessed 4 June 2022].
- [22] European Commission, “Coordinated Plan on Artificial Intelligence 2021 Review,” European Commission, 21 April 2021. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>. [Accessed 31 May 2022].
- [23] European Commission, “Communication from the Commission to the European Commission, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Coordinated Plan on Artificial Intelligence,” 7 December 2018. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0002.02/DOC_1&format=PDF. [Accessed 31 May 2022].
- [24] Council of the EU, “Conclusions on the Coordinated Plan on Artificial Intelligence,” 11 February 2019. [Online]. Available: <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf>. [Accessed 31 May 2022].
- [25] European Commission, “A European Approach to Artificial Intelligence,” European Commission, 23 February 2022. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/news/commission-invest-eu292-million-digital-technologies-and-cybersecurity>. [Accessed 3 June 2022].
- [26] European Commission (EPSC), “The Age of Artificial Intelligence: Towards a European Strategy for Human-Centric Machines,” Publications Office of the European Union, 25 November 2019. [Online]. Available: <https://op.europa.eu/en/publication-detail/-/publication/f22f6811-1007-11ea-8c1f-01aa75ed71a1/language-en>. [Accessed 3 June 2022].
- [27] US Congress, “Public Law No: 116-283 (01/01/2021). William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,” 3 December 2020. [Online]. Available: <https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210>. [Accessed 3 June 2022].
- [28] European Parliament, “China’s Ambitions in Artificial Intelligence,” 9 September 2021. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA\(2021\)696206_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA(2021)696206_EN.pdf). [Accessed 3 June 2022].
- [29] Government of the United Kingdom, “National AI Strategy,” September 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf. [Accessed 3 June 2022].

- [30] Ministry of Economy, Trade and Industry of Japan (METI), “AI Governance in Japan Ver. 1.0,” 15 January 2021. [Online]. Available: https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_4.pdf. [Accessed 3 June 2022].
- [31] Canadian Institute for Advanced Research (CIFAR), “Pan-Canadian AI Strategy Impact Assessment Report,” October 2020. [Online]. Available: <https://cifar.ca/wp-content/uploads/2020/11/Pan-Canadian-AI-Strategy-Impact-Assessment-Report.pdf>. [Accessed 3 June 2022].
- [32] J. Stempel, “Face Scanner Firm Clearview AI Agrees to Limits to Settle Lawsuit,” Reuters, 9 May 2022. [Online]. Available: <https://www.reuters.com/technology/face-scanner-firm-clearview-ai-agrees-limits-settle-lawsuit-2022-05-09/>. [Accessed 3 June 2022].
- [33] K. Drinhausen and V. Brussee, “China’s Social Credit System in 2021: From Fragmentation towards Integration,” 3 March 2021. [Online]. Available: <https://merics.org/sites/default/files/2022-05/MERICS-China-Monitor67-Social-Credit-System-final-4.pdf>. [Accessed 3 June 2022].
- [34] Special Committee on Artificial Intelligence in a Digital Age (AIDA), “Report on Artificial Intelligence in a Digital Age,” 22 March 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.pdf. [Accessed 4 June 2022].
- [35] European Commission, “Digital in the EU-US Trade and Technology Council,” European Commission, 16 May 2022. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council>. [Accessed 3 June 2022].
- [36] European Commission, “EU-US Trade and Technology Council: Strengthening our Renewed Partnership in Turbulent Times,” European Commission, 16 May 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3034. [Accessed 3 June 2022].
- [37] EP Committee on the Internal Market and Consumer Protection and EP Committee on Civil Liberties, Justice and Home Affairs, “Draft Report on Artificial Intelligence Act,” 20 April 2022. [Online]. Available: https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf. [Accessed 17 June 2022].
- [38] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (GDPR),” 25 January 2012. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN>. [Accessed 13 June 2022].
- [39] A. Balocchi, “L’Europa al lavoro per ultimare l’AI Act,” Tech4Future, 5 April 2022. [Online]. Available: <https://tech4future.info/regolamento-ue-intelligenza-artificiale-2022/>. [Accessed 21 June 2022].

Annex II The relationship between LEAs and commercial actors

General overview

Over the years, and particularly since the end of the Cold War, there has been in the West, and particularly in the Anglo-Saxon world (lately spread also to other European countries and other regions of the world), a triumph of neo-liberal policies in the economic sphere, as well as major privatisation processes of companies that were previously state-controlled [1]. These privatisations have gradually reached even strategic sectors for the state, such as defence and intelligence activities, once the heart of the regal functions of the state.

Hence, there has been a shift from a situation where the state was in charge of all intelligence activities to the present time, where the state has delegated many of its functions, including in the field of intelligence and defence.

The case of the United States, where the privatisation of national security (i.e. intelligence but also national defence) has been taken so far that many intelligence activities are carried out by private companies, is often seen as a forerunner in this field.

The privatisation of intelligence in the United States was first of all part of a particular political context. Following the end of the Cold War, Presidents Bill Clinton and then George W. Bush both supported a neo-liberal economic logic according to which the privatisation of certain state functions could offer a solution to the lack of resources, capacities and efficiency of the public sector. In the 1990s, this logic was applied to the defence and national security sectors (i.e. also to the US intelligence community) at the same time as their budgets were drastically reduced. Thus, the number of civil servants in this field decreased sharply while the number of contractual agents in charge of secondary tasks increased [2]. Moreover, the changing nature of the threats facing the US government since the end of the Cold War requires increasing coordination and integration between the public and private sectors. For example, the ability of the terrorist threat to penetrate liberal societies and its indiscriminate targeting of civilians requires greater integration between the government and civilian entities - including businesses - that may be subject to terrorist attack [3].

Finally, the intensification of public-private relations in this field is explained by the fact that the private sector has become quite indispensable for those seeking a technological advantage. Public services, however extensive, will hardly be able to match the pool of knowledge and capabilities developed and maintained by the private sector.

In fact, these services now cover the full range of intelligence activities (collection, analysis, administrative support and training, dissemination, counter-intelligence and covert operations). The reservoir of knowledge and capabilities available to companies should encourage any government to explore the relationship between intelligence services and companies as a support for intelligence.

In the 21st century, the intensification of public-private relations in the intelligence sector seems inevitable if competitive intelligence services are to be maintained. However, these relationships are bound to develop in a market characterised by imperfect competition. It is therefore necessary for the state to pay particular attention to the control of this market in order to mitigate the most negative aspects of its outsourcing and to maintain a hierarchy between public authority and the private sector [4].

What is happening in Europe (apart from Great Britain, which in some ways has followed a trajectory more similar to that of the United States for some time now) is that such massive delegation of intelligence activities to private companies has not yet taken place.

In Europe, in fact, some functions are still seen as uniquely incumbent on the state. In France, we are witnessing the emergence of Private Military Companies (PMCs), a prodrome of the privatisation of intelligence.

The phenomenon of PMCs began rather recently, and in particular after the fall of the USSR, although even earlier some states had recourse to the help of private companies for the transport of arms, personnel or more generally in logistics, as was the case for the USA during the Vietnam War. This recourse remained exceptional and very limited in time. Moreover, what characterised these recourse in the past was the absence of this military or security aspect outside the state field, as these companies did not have the right to resort to the use of violence.

However, PMCs have been able to seize political and economic windows of opportunity to expand their field of competence. Thus, in the 1990s, we went from timid logistical support actions (transport of equipment, maintenance, handling) and a few demining actions (Mozambique, Angola and Cambodia) to a rapid expansion of the fields of action, such as military training, communication, technical support, up to certain cases (Sierra Leone and Angola) where we witnessed a direct participation of the PMCs in the conflicts, but which was nevertheless very contested [5].

The 2001 attacks on American soil and the renewal of security legislation have given a new impetus to these PMCs, which have seen their spectrum of action significantly broadened. The use of force and violence have thus become legitimate means of action for these PMCs. The PMCs have grown so much that until a few months ago in Afghanistan the ratio of contractors (one of the terms used to indicate PMC members/employees) to regular US army soldiers was unfavourable to the latter [6].

Nowadays, not only States, but also the United Nations and more generally the large international organisations as well as companies are increasingly calling on these PMCs. "*New operators of private violence, private security companies propose the implementation, through a contractual and legal process, of various forms of physical constraint, outside their national territory. They thus offer their clients armed services [...] or less controversial services*" [7].



Private Military Companies and State of ownership

The emergence of PMC is to some extent the result of the dominant neo-liberal policies at the international level, which have resulted in profound changes in the very essence of the state and its functions. Thus we

observe that even a regalian function of the state, which is also historically linked to the formation of the state, that of the monopoly of violence, is not exempt from renewal. We are not entering into the debate that opposes the academic world between, on the one hand, those who insist that this would be a clear sign of a withdrawal of the state, of a loss of control even over the essential functions that characterise it and, on the other hand, those who say that, in the end, it would only be a matter of a renewal and redeployment of the state whose regalian functions would not be called into question. What we observe is that this 'privatisation of regalian functions' and the use of PMCs is a growing reality.

It should be added, however, that these PMCs respond in some ways to more general changes in the way war is waged, which is increasingly within states rather than between states. This in no way implies a weakening of the internationalisation of certain conflicts at first sight within a single state, which is not really paradoxical. We are simply witnessing new configurations of armed conflicts in which new actors are emerging. The general trend seems to be both the 'privatisation of mercenarism' and the mercenarisation of warfare, which is increasingly carried out by proxy. The growing role of PMCs, their increasingly frequent use and the widening scope for the use of violence imposes new legal challenges, in particular with regard to International Humanitarian Law (IHL).

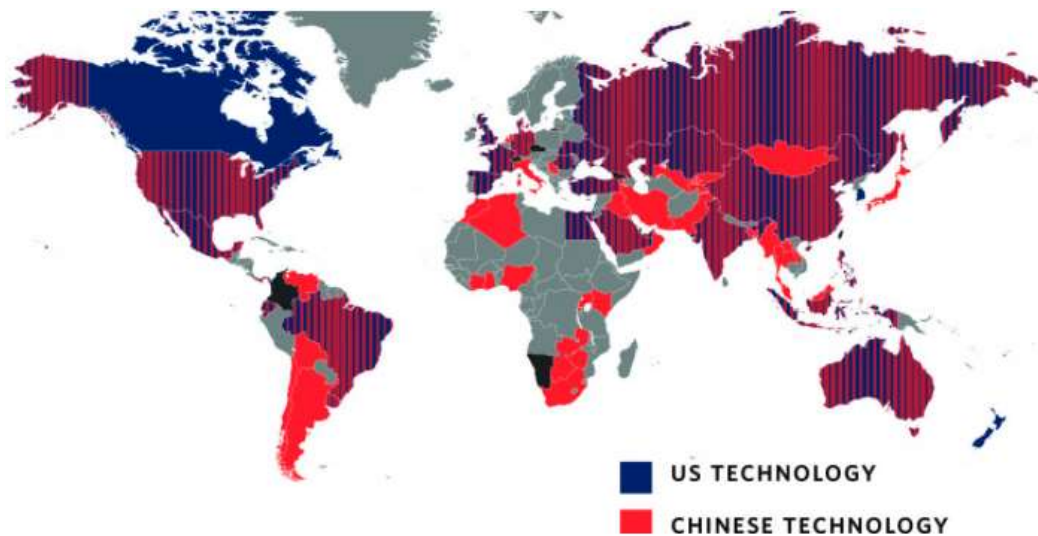
In Europe, however, there is still no talk of the privatisation of intelligence, but only of the use of external actors in some cases. There is also a substantial difference between police and surveillance actions in the local sphere and those carried out in the international sphere and which risk interfering with national security. In many cases in Europe, the police have already outsourced some of their functions, for instance by contracting out phone tapping to external companies, especially when it comes to crimes committed within the national territory. In this sense, the police delegate to accredited private companies some of the work that they used to do in the past, keeping only the analysis of the data told by an external company for themselves.

Nevertheless, some LEAs find themselves working at different levels with commercial companies, e.g. with regard to software, type of technology purchased, data processing or analysis, etc. The main problems that an LEA may encounter when using the work of a private actor may be the following:

1. type and ownership of the technologies used;
2. accountability and responsibility of private companies;
3. legal framework in which operations are carried out.

1. Type and ownership of the technologies used

One of the first problems LEAs face when they have to use the commercial services of technology providers is the very origin of the technologies they would like to use (and not the reseller who markets them). In fact, while some relationships with states outside the EU are not really collaborative in the strategic sphere (such as national security), the relationship is purely commercial when it comes to technologies. From this point of view, in the technologies used by LEAs, Europe is rarely the producer and supplier of these technologies, but the ultimate user. European states, in this sense, mainly use Chinese and American technologies [8].



Countries using US and Chinese technologies for surveillance activities

For the LEAs, the purchase of a technology from one state or another is not a matter of purely commercial logic, as other considerations come into play, such as the assessment of dependence on technologies from more technologically advanced allied countries - such as the United States - or from countries that offer excellent solutions at competitive prices but are not allies, opening up the possibility of being objects of espionage or of being technologically dependent on non-allied countries that might in the future have more hostile policies, such as China.

2. Accountability and responsibility of private companies

When LEAs work with private companies, there are various issues. If the private company is only the provider of the technology, the responsibility for the action taken lies with the LEAs, and thus with the state. If, on the other hand, LEAs have delegated a mandate to a private company, the accountability and responsibility situation changes. If an LEAs delegates a type of work to a private company, there are a number of issues, including the types of information that the LEA has to give to the private company, how the data is analysed and transmitted, the ownership and use of that information, the vulnerability of the information itself, the possibility of a leakage of information, the vulnerabilities of the technologies used by the private companies themselves doing work on behalf of the LEAs.

A whole other set of issues come from the ways in which the performance of private companies working on behalf of LEAs and their effectiveness can be assessed, as well as the problem of direct control of operations. In addition, another issue is that of the legal framework in which private companies operate.

For instance, in the case of a 'simple' wiretap in case there is a suspicion of a crime, many European states' laws require LEAs to carry out wiretaps under a mandate from the competent judicial authority. In some cases, however, LEAs may give a mandate to private companies, which act on behalf of the LEAs, to perform these interceptions [9]. In this case, all the questions and problems addressed in this section become a reality.

3. Legal framework

When LEAs find themselves acting, particularly in the intelligence domain and when it comes to national security, there are principles and national legislation to be followed. In this regard, some the most important principles could find in the "International Standard of Good practices for the promotion of Human Rights and fundamental freedoms while countering terrorism" established by the United Nations.

International Standard of Good practices for the promotion of Human Rights and fundamental freedoms while countering terrorism

Mandate and legal basis	
Practice 1	Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyze and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.
Practice 2	The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.
Practice 3	The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.
Practice 4	All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.
Practice 5	Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.
Oversight institutions	
Practice 6	Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.
Practice 7	Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.
Practice 8	Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.
Complaints and effective remedy	
Practice 9	Any individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.
Practice 10	The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are independent of the intelligence services and the political executive. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.
Impartiality and non-discrimination	

Practice 11	Intelligence services carry out their work in a manner that contributes to the promotion and protection of the human rights and fundamental freedoms of all individuals under the jurisdiction of the State. Intelligence services do not discriminate against individuals or groups on the grounds of their sex, race, color, language, religion, political or other opinion, national or social origin, or other status.
Practice 12	National law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.
Practice 13	Intelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression.
State responsibility for intelligence services	
Practice 14	States are internationally responsible for the activities of their intelligence services and agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services.
Individual responsibility and accountability	
Practice 15	Constitutional, statutory and international criminal law applies to members of intelligence services as much as it does to any other public official. Any exceptions allowing intelligence officials to take actions that would normally violate national law are strictly limited and clearly prescribed by law. These exceptions never allow the violation of peremptory norms of international law or of the human rights obligations of the State.
Practice 16	National laws provide for criminal, civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations.
Practice 17	Members of intelligence services are legally obliged to refuse superior orders that would violate national law or international human rights law. Appropriate protection is provided to members of intelligence services who refuse orders in such situations.
Practice 18	There are internal procedures in place for members of intelligence services to report wrongdoing. These are complemented by an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate. Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern.
Professionalism	
Practice 19	Intelligence services and their oversight institutions take steps to foster an institutional culture of professionalism based on respect for the rule of law and human rights. In particular, intelligence services are responsible for training their members on relevant provisions of national and international law, including international human rights law.
Human rights safeguards	
Practice 20	Any measures by intelligence services that restrict human rights and fundamental freedoms comply with the following criteria: <ul style="list-style-type: none"> - They are prescribed by publicly available law that complies with international human rights standards; - All such measures must be strictly necessary for an intelligence service to fulfil its legally prescribed mandate; - Measures taken must be proportionate to the objective. This requires that intelligence services select the measure that least restricts human rights, and take special care to minimize the adverse impact of any measures on the rights of individuals, including, in particular, persons who are not suspected of any wrongdoing; - No measure taken by intelligence services may violate peremptory norms of international law or the essence of any human right; - There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights;

	- Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy.
Intelligence collection	
Practice 21	National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorizing, overseeing and reviewing the use of intelligence- collection measures.
Practice 22	Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence-collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.
Management and use of personal data	
Practice 23	Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.
Practice 24	Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.
Practice 25	An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.
Practice 26	Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information.
The use of powers of arrest and detention	
Practice 27	Intelligence services are not permitted to use powers of arrest and detention if they do not have a mandate to perform law enforcement functions. They are not given powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities.
Practice 28	If intelligence services have powers of arrest and detention, they are based on publicly available law. The exercise of these powers is restricted to cases in which there is reasonable suspicion that an individual has committed or is about to commit a specific criminal offence. Intelligence services are not permitted to deprive persons of their liberty simply for the purpose of intelligence collection. The use of any powers and arrest and detention by intelligence services is subject to the same degree of oversight as applies to their use by law enforcement authorities, including judicial review of the lawfulness of any deprivation of liberty.
Practice 29	If intelligence services possess powers of arrest and detention, they comply with international human rights standards on the rights to liberty and fair trial, as well as the prohibition of torture and inhuman and degrading treatment. When exercising these powers, intelligence services comply with international standards set out in, inter alia, the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, the Code of Conduct for Law Enforcement Officials and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.
Practice 30	Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.

Intelligence sharing and cooperation	
Practice 31	Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.
Practice 32	National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.
Practice 33	Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.
Practice 34	Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.
Practice 35	Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.

In some EU member states, intelligence services are further divided into separate departments related to domestic security and foreign intelligence, or according to specific themes. In practice, however, due in part to the overlapping and blurring of activities and responsibilities, the line separating these bodies is increasingly ambiguous [10]. One need only think of the fact that certain digital techniques such as telephone interception, spyware, or geolocation of mobile devices are currently used by both military and civilian intelligence. The data collected are then sometimes uploaded to common platforms accessible to several services at the same time, even those not belonging to the services and participating more or less directly in certain operations, such as those against organized crime, corruption or terrorism.

One of the other problems of collaboration between LEAs and private commercial actors, especially when there is information that is sensitive or that concerns national security, relates to the handling of data by private companies when they are entrusted with work on behalf of LEAs.

Private companies could in fact be led either to obtain information on behalf of LEAs (the most frequent scenario) and then pass it on in an encrypted manner to LEAs. In this case, the most serious issues concern a possible cloud for sharing data and the vulnerabilities of the data itself.

If, on the other hand, private companies were to do data analysis on behalf of the LEAs, in addition to the problems already outlined above, there would also be the problem of data ownership and management, especially confidential information, which, due to the fact that it is also held by third parties, is more vulnerable. When it comes to national security issues, in addition to periodic national authorisations and certifications, LEAs tend not to want to take risks and delegate activities.

References

[1] I. W. Lieberman, "Privatization: the Theme of the 1990s," *The Columbia Journal of World Business*, vol. 28, no. 1, pp. 8-17, 1993.

- [2] C. I. Agency, «Statement by the Director of Central Intelligence Regarding the Disclosure of the Aggregate Intelligence Budget for Fiscal Year 1998,» [Online]. Available: <https://www.cia.gov/news-information/press-releases-statements/press-release-archive-1998/ps032098.html>.
- [3] D. V. Puyvelde, «Quelles leçons tirer de la privatisation du renseignement aux États-Unis ?,» *Revue internationale et stratégique*, vol. 3, n. 87, pp. 42-52, 2013.
- [4] S. Chesterman, «‘We Can’t Spy ... If We Can’t Buy!’: The Privatization of Intelligence and the Limits of Outsourcing ‘Inherently Governmental Functions’,» *The European Journal of International Law*, vol. 19, n. 5, 2008.
- [5] S. P., «Soldats privées,» *Études*, n. 4, pp. 452-462, 2008.
- [6] P. Walter, «Up to 56,000 more contractors likely for Afghanistan, congressional agency says,» 16 12 2009. [Online]. Available: <https://www.washingtonpost.com/wp-dyn/content/article/2009/12/15/AR2009121504850.html?hpid=topnews&noredirect=on>. [Last accessed 26 09 2022].
- [7] M.-p. C., «Des mercenaires aux compagnies de sécurité privée. Construction et pratique de légitimation de la violence privée commerciale dans le système international,» *Déviance et Société*, vol. 37, n. 4, pp. 487-508, 2013.
- [8] F. Steven, «Carnegie Endowment for International Peace,» 19 09 2019. [Online]. Available: <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>. [Last accessed 3 10 2022].
- [9] Axerta, «Intercettazioni telefoniche,» 3 3 2019. [Online]. Available: <https://www.axerta.it/intercettazione-telefonica/#:~:text=1.,intercettazione%20con%20un%20decreto%20motivato..> [Last accessed 3 10 2022].
- [10] E. U. A. f. F. Rights, «Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, volume 1 and volume 2,» 2015. [Online]. Available: <https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-s>. [Last accessed 3 10 2022].

Annex III Trustworthiness of the AI

Abstract

The rapid development of artificial intelligence (AI) technology has made it possible to create various systems based on it. However, as practice shows, many modern artificial intelligence systems are vulnerable to stealth attacks, in some aspects biased and lacking protection of user privacy. These shortcomings represent all artificial intelligence systems from the negative side to the end users. This report provides data on how to build and maintain robust AI systems. Report presents the theoretical framework for important aspects of AI reliability, including reliability, generalization, explainability, transparency, reproducibility, fairness, privacy, and accountability. Key opportunities and challenges for the design and development of robust AI systems are also briefly reviewed.

Introduction

The rapid development of artificial intelligence (AI) continues to bring significant economic and social benefits to society. As the involvement of AI in areas such as transportation, finance, medicine, security and entertainment increases, society realizes the high importance of the reliability of such systems. This is because there could be serious social consequences – due to the loss of stakeholder confidence in such systems (given the prevalence of these AI systems).

In the AI community (researchers, developers, and decision makers), it is common to consider system performance (i.e., accuracy) as the primary measure of their workflows. This metric is far from enough to reflect the robustness of AI systems. In addition to the performance of an AI system, to improve its reliability, various aspects of such systems should be considered, for example, their reliability, algorithmic fairness, explainability, and transparency.

While the most active academic research into AI reliability has focused on the algorithmic properties of models, advances in algorithmic research alone are not enough to create robust AI products. From an industrial point of view, the life cycle of an AI product consists of several stages, namely:

- data preparation,
- algorithm design,
- development and deployment
- operation,
- monitoring
- control.

Improving reliability in any single aspect involves efforts at several stages of this life cycle, such as data cleansing, robust algorithms, anomaly monitoring, and risk auditing. On the contrary, a breach of trust in any single link or aspect can undermine the reliability of the entire system. Therefore, the reliability of AI should be established and systematically assessed throughout the life cycle of an AI system.

In addition to a holistic view of the reliability of AI systems at all stages of their life cycle, it is important to understand the big picture of the various aspects of AI reliability. In addition to ensuring the reliability of AI by establishing requirements for each specific aspect, it is worth noting the combination and interaction between these aspects, which are important and little-studied topics for reliable real-world AI systems.

The simple combination of systems to improve each aspect of reliability separately does not guarantee a more reliable and efficient end result. Instead, thoughtful joint optimization and trade-offs between several aspects of reliability are needed [1, 2, 3, 4, 5].

A new approach is needed to move AI technologies from the performance plane to the reliability plane. This requires conscientiousness on the part of representatives of various disciplines and interdisciplinary and cooperation when working on various aspects of reliability and at different stages of the system life cycle.

Existing developments in the field of artificial intelligence can be grouped either from the standpoint of scientific research [6, 7, 8], or engineering [9, 10, 11, 12, 13]. Developments from related non-technical fields also include manuals [14, 15, 16], standardization [17], and management processes [18, 19, 20].

Trustworthiness of artificial intelligence

The success of machine learning technology in recent decades is largely dependent on performance measurements based on accuracy. By evaluating task performance based on quantitative accuracy or loss, AI training models become manageable in terms of optimization. Meanwhile, predictive accuracy is widely used to denote the superiority of an AI product over others. However, with the recent widespread use of AI, limiting measurement to accuracy alone has faced a number of new challenges, ranging from malicious attacks on AI systems to misuse of AI that violates human values. To address these issues, the AI community has realized over the past decade that when building an AI system, facts beyond precision, such as reliability, security, transparency, and fairness, should be taken into account and improved [14].

Reliability

Reliability refers to the ability of an algorithm or system to deal with runtime errors, erroneous inputs, or invisible data. Reliability is an important factor influencing the performance of AI systems under empirical conditions. Lack of reliability can also lead to unintended or harmful system behavior. When considering ML systems, the term "reliability" can be applied in various situations. The report examines vulnerabilities at the data, algorithm, and system levels, respectively.

Data. As the use of AI systems increases, the environment in which the AI model is deployed becomes more complex and diverse. If an AI model is trained without taking into account the different distributions of data in different scenarios, its performance can suffer significantly. Robustness to distribution shifts has been a common problem in various AI applications [21].

Algorithms. It is a well-known fact that AI models can be vulnerable to attack by malicious attackers. In recent years, among the various forms of attacks, a serious challenge for the industry and theoretical researchers has been the adversarial attack and defenses against it. In publications, the threat of enemy attack is classified according to several typical aspects and various approaches to protection are proposed [22, 23, 24, 25, 26]. For example, in [27] attacks from the enemy were classified by the time of the attack. A decision-time attack skews the input samples to mislead the prediction of a given model so that an attacker can evade security checks or impersonate victims. A poisoning attack is a training-time attack in which carefully designed patterns are introduced into the training data in order to change the system's response to certain patterns. Given the practicality of the attacks, it is also useful to note the differences between the attacks in terms of the spaces in which they are executed. Traditional research has mainly focused on feature space attacks that are generated directly as model input features. In many practical scenarios, attackers can only modify the input object in order to indirectly create features related to the attack. Research into creating realizable object-based attacks (problem attacks) has recently received increased interest [28, 29]. Algorithm-level threats can exist in a variety of forms beyond directly misleading AI models. Model theft (also known as exploratory attack) attempts to steal knowledge about models. While this does not directly change the behavior of the model, the stolen knowledge goes a long way in generating hostile samples [30].

Systems. In realistic AI products, system-level resilience to illegal activities should also be carefully considered.

There are various approaches to prevent vulnerabilities in AI systems. The goal of protection can be either proactive or reactive [31]. Proactive defense attempts to optimize the AI system to be more resilient to various inputs, while reactive defense aims to detect potential security issues such as changing distributions or hostile samples.

Assessing the reliability of an AI system is an important means of preventing vulnerabilities and controlling risks. Let us briefly consider two groups of evaluations: the robustness test and the mathematical verification. Test of endurance. Testing serves as an important approach to evaluating and improving the reliability of not only conventional software, but also AI systems. Traditional functional testing techniques such as the monkey test [32], provide efficient approaches to assessing system-level reliability. Software testing methodologies have recently been extended to assess resilience to adversary attacks [33, 34].

Compared to functional testing, performance testing, i.e. benchmarking, is a more common approach in the field of machine learning to evaluate the performance of a system in various parameters. Machine learning studies use test datasets with different distributions to evaluate data reliability. In the context of hostile attacks, the minimum hostile perturbation is the main reliability metric, and its empirical upper bound, also known as empirical reliability [35, 36]. From an attacker's point of view, the success rate of an attack also intuitively measures the reliability of a system [35].

Mathematical verification is a certified verification of the resistance of an AI model to adversarial actions, inherited from the theory of formal methods.

Generalization

Generalization is the ability to extract knowledge from limited training data in order to make accurate predictions about unseen data [37].

On the one hand, generalization requires AI systems to make predictions on realistic data, even in areas or distributions they are not trained on [37]. This significantly affects the risk of practical systems and their reliability. On the other hand, AI models should be able to generalize without having to exhaustively collect and annotate large amounts of data for various domains [38, 39]. This improves the stability and affordability of AI system deployments across a wide range of applications.

Creating a modern data-driven AI model requires a large amount of data and annotations during the training phase. This leads to high costs for manufacturers and users to re-collect and re-annotate data to train the model on each task. The cost highlights the need to generalize knowledge about the model for different tasks, which not only reduces the cost of the data, but in many cases improves the performance of the model. One of the most popular approaches for evaluating the generalization of an AI model in realistic scenarios is a comparative analysis of test datasets with different distributions. A summary of commonly used datasets and domain generalization tests can be found in [38]. There, the tasks of object recognition, actions, segmentation and face recognition are considered.

Explainability and transparency

The opacity of complex AI systems has caused widespread concern in academia, industry, and society at large. In terms of practical systems, there is a demand among users for the right to know the intent, business model, and technological mechanism of AI products [40, 41]. A number of studies have addressed these issues in terms of nomenclature, including interpretability, explainability, and transparency [42, 43, 5, 44, 45, 46], and delved into various definitions.

Explainability, that is, understanding how an AI model makes decisions, remains at the center of current AI research and is a fundamental factor in determining the credibility of AI technology. The motivation for explainability of AI comes from different aspects [47, 42]. From a scientific research point of view, it is important to understand all the internal mechanisms of data, parameters, procedures, and results in an AI system. From the point of view of creating AI products, there are various practical requirements for explainability. For operators, such as bank executives, explainability helps to understand the AI credit system in order to prevent its potential defects [47, 48]. Users such as loan applicants are interested to know why the model is rejecting them and what they can do to qualify [47].

One of the most active areas of work in the field of machine learning are approaches to explainability, which have been comprehensively considered in various studies [42, 43, 5, 45].

It is worth noting that the unified assessment of explainability has been recognized as a challenging task. The main reason for this lies in the ambiguity of the psychological description of explainability. To circumvent this problem, various studies have used qualitative measures to assess human explainability. (opinions, self-reports, questionnaires and case studies that measure e.g. user satisfaction, subjective evaluation of a person). Evaluation such as the performance of human tasks and AI can be used to develop, for example, recommendation systems [49] and data analysis [50])

Despite the above estimates, direct quantitative measurement of explainability remains a challenge. A recent study on the complexity of machine learning models [51] and their cognitive - functional complexity [52] has opened a avenue for future research to find a unified metric for quantification.

Transparency requires disclosure of system information and has long been a recognized requirement in software development [53, 54]. In the AI industry, this requirement naturally spans the lifecycle of an AI system and helps stakeholders confirm that it reflects the appropriate design principles. Overall, transparency is a key requirement for building public trust in AI systems [14, 55, 56].

To make the life cycle of an AI system transparent, it is necessary to disclose various information about its creation, including design goals, data sources, hardware requirements, configurations, operating conditions, expected use and system performance. Recently appeared The rise of open source systems is also making a significant contribution to the algorithmic transparency of AI systems.

For an interactive AI system, a well-designed user interface serves as an important means of revealing the underlying decision-making procedure [57].

Although a single quantitative assessment is not yet available, the qualitative assessment of transparency has undergone recent developments in the AI industry. Checklists for evaluation [57, 58] are considered an effective tool for evaluating and increasing the transparency of the system. In the context of user psychology or the public, user research or A/B tests can provide a useful assessment based on user

Reproducibility

Modern AI research includes both mathematical inference and computational experiments. The reproducibility of these computational procedures serves as an important step in validating AI research. In terms of AI reliability, this check facilitates the detection, analysis and mitigation of potential risks in the AI system, such as the vulnerability of certain inputs or unintentional bias.

Reproducibility not only provides effective verification of research results, but also allows the community to quickly apply the latest approaches in practice or conduct additional research. There is a new trend in scientific circles to consider reproducibility as a requirement when publishing studies [59].

In recent machine learning reproducibility studies, this requirement has been decomposed into reproducibility of data, methods, and experiments [59, 60, 61], where the latter cover a range of lifecycle artifacts such as code, documentation, software, hardware, and deployment configuration. Based on this methodology, more and more machine learning frameworks are being developed to help researchers and developers better track the lifecycle in a reproducible manner [61, 62].

Justice

The overall goal of fairness in AI systems is to remove or mitigate the effects of biases.

Bias can take various forms, such as data bias, model bias, and procedure bias in the development and application of AI systems [63].

Group identity (sometimes also called sensitive variables) and system response (prediction) are two factors influencing bias. In some cases, objective ground truths of the given task are also used, which should be taken into account when evaluating the fairness of the system, for example, whether the speech of a person is correctly recognized or whether his face is correctly identified.

Fairness can be applied to many details of system behavior [63, 64, 65]. At each level of detail, the indicator of interest is fairness of distribution or fairness of the result, procedural fairness or fairness of the process [66]. In each case, the aggregate behavior and bias in it of the AI system is of interest, which is called statistical fairness or group fairness. In some applications, it is also useful to consider individual fairness or counterfactual fairness, especially when the sensitive variable is more easily separated from other characteristics that should reasonably determine the system's prediction [63].

While the former is more widely applicable to various machine learning tasks such as speech recognition and face identification, the latter can be critical in cases such as reviewing resumes to screen candidates [67].

At the group level, researchers have identified three abstract principles for classifying different types of justice [64].

Privacy Protection

Privacy protection mainly refers to the protection against unauthorized use of data that can directly or indirectly identify a person or household. This data covers a wide range of information, including name, age, gender, facial image, fingerprints, etc. Commitment to protecting privacy is considered an important factor in determining the reliability of an AI system.

The recently released AI ethics guidelines also highlight privacy as one of the key concerns [14, 40].

The General Data Protection Regulation (GDPR) is a representative legal framework that encourages businesses to take effective measures to protect user privacy.

Existing protection methods cover the entire life cycle of artificial intelligence systems to address growing privacy concerns.

In practical scenarios, an empirical assessment of the risk of leakage of confidential information is usually considered [68, 69].

Accountability: a holistic assessment of the above requirements

Accountability is about regulating AI systems to meet these requirements. With the gradual improvement of AI governance legal and institutional norms, accountability is becoming a critical factor for AI to sustainably benefit society through credibility [70].

Accountability runs through the entire life cycle of an AI system and requires that the stakeholders of an AI system are required to justify their design, implementation and operation in accordance with human values. In terms of disclosure, transparency contributes to the main mechanism used to facilitate the accountability of the AI system [70, 71].

From accountability also follows the concept of verifiability, which requires the justification of the system to be analyzed, evaluated and audited [72]. Algorithmic auditing is a widely accepted approach to holding an AI system accountable and evaluating its impact on multiple aspects of human values [73].

Deployment

Once developed, AI systems are deployed on realistic products and interact with the environment and users. To ensure the reliability of systems, a number of approaches should be considered during the deployment phase, such as adding additional components for anomaly tracking and developing specific human-AI interaction mechanisms to ensure transparency and explainability.

Anomaly monitoring . Anomaly monitoring methodology has proven itself in software development. For AI systems, the range of monitoring has been further extended to cover data outliers, data drift, and model

performance. As a key measure for the success of an AI system, monitoring provides the means to improve system reliability in many ways. Some representative examples are discussed below.

Attack monitoring is widely used in traditional SaaS, such as fraud detection [74] in e-commerce systems.

Data drift monitoring [75] provides an important means to maintain the generalization of an AI system when the concept changes [76] caused by a dynamic environment such as market change [77]. Misuse monitoring has also recently been adopted in several AI cloud services [78] to avoid misuse such as unauthorized surveillance of the population or individual tracking through facial recognition, which helps ensure that ethical values are properly aligned.

Human-AI Interaction As an extension of human-computer interaction (HCI), human-AI interaction has received widespread attention in the AI industry [79, 80]. Effective human-AI interaction affects the robustness of an AI system in many ways.

The user interface serves as the most intuitive factor influencing the user experience. For an AI system, this is the main means of revealing internal information and decision-making procedures to users, which has an important impact on the transparency and explainability of the system [18, 81]. There are various interaction approaches to improve the explainability of AI, including the visualization of machine learning models [82] and interactive settings [81]. In addition to being transparent and explainable, the accessibility of an interface also has a significant impact on user trust. AI-based interaction technologies enable the creation of various new forms of human-machine interfaces, such as chatbots, audio speech recognition, and gesture recognition. This can lead to accessibility issues for people with disabilities and requires full consideration [83, 84].

Failover Mechanisms. Given the imperfections of existing artificial intelligence systems, it is important to avoid causing harm when the system fails in exceptional cases. While studying traditional real-time automation systems, the AI community realized that a fail-safe mechanism or fallback plan should be an integral part of the design of an AI system if its failure could cause harm or loss. This mechanism is also becoming an important requirement in recent AI manuals such as [40]. Over the past few years, fail-safe design has been seen in many areas of robotics. In the field of UAVs, a fault-tolerant algorithm has been studied for a long time to avoid frequent collisions of quadcopters. [85] and ensure a safe landing in the event of system failure [86].

Hardware security. AI systems are widely deployed on a variety of hardware platforms to handle a variety of scenarios ranging from servers in data centers to mobile phones and embedded systems. Attacks on OS and hardware introduce new risks, such as data falsification or theft, and threaten the reliability, security, and privacy of AI systems. Various approaches have been explored to deal with this new threat [87]. From a hardware security perspective, the concept of Trusted Execution Environment (TEE) is a recent representative technique that has been adopted by many hardware vendors [88]. The general mechanism of TEE is to provide a safe area for data and code. The standard OS does not interfere in this area, so a protected program cannot be attacked. ARM processors support TEE implementation using the TrustZone scheme [89]. They run a secure OS and a normal OS at the same time on the same core. The secure part provides a secure environment for sensitive information. Intel Extensions Software Guard Extensions (SGX) implement TEE through hardware-based memory encryption [90]. Its enclave mechanism allows you to allocate secure memory to store private information. Such security mechanisms have been used to protect sensitive information such as biometric identifiers and financial account passwords and are applicable to other AI use cases.

Cooperation and exchange of information. Building robust AI requires collaboration between stakeholders. From an industry perspective, collaboration with academia enables new technologies to be quickly applied to improve product performance and reduce product risk. Cooperation with regulatory bodies certifies products as complying with the principles of reliability. In addition, collaboration between industries helps to solve consensus-based problems such as data sharing, standardization, and ecosystem building [91]. Recent

AI stakeholder practices have shown the effectiveness of collaboration in various ways. We summarize these practices in the following aspects below.

Reliable data exchange. The growing value of data for business increases the need to share it between companies in different scenarios (for example, a medical AI system). In addition to privacy-based computing, collaboration between data owners, technology providers and regulators is moving forward in building a data sharing ecosystem and addressing issues such as data pricing and data authorization.

Joint development of regulation. Active participation in the development of standards and regulations provides an important means for academia, industry and regulators to align their requirements and situations.

Exchange of incidents. The AI community has recently recognized incident sharing as an effective approach to identify and mitigate potential risks to AI systems [10]. AI incident database [92] provides an example for stakeholders to share negative AI incidents so that the industry can avoid similar issues.

Conclusions

First of all, it is important to note the importance of shifting the focus from performance-oriented AI to trust-oriented AI. In the short term, this shift will inevitably have side effects such as increased training time, slower development, and/or increased cost of building AI systems. However, we encourage practitioners to focus on the long-term benefits of gaining the trust of all stakeholders for the sustainable use and development of these systems.

AI reliability as a long-term study. The current understanding of AI reliability is far from complete or universal and will inevitably evolve as new AI technologies will be developed and an understanding of their impact on society will be more clearly formed. This procedure requires long-term research.

Immaturity of approaches to trustworthiness. Some aspects of AI robustness, such as explainability and robustness, address the limitations of current AI technologies. Despite the widespread interest in AI research, satisfactory solutions are still far from being achieved.

The arms race between adversary offense and defense reflects the immaturity of our understanding of AI reliability. As in other areas of security, attacks evolve as defenses evolve. It has been shown that conventional adversarial training [93] is easily fooled by subsequent attacks [94]. It was later shown that the corresponding defense [94] is vulnerable to new attacks [95]. This not only requires practitioners to be flexible in adopting defensive techniques to reduce the risk of new attacks in a process of long-term and ongoing development, but also poses long-term challenges for theoretical research [96].

Increasing transparency increases trust in AI systems through information disclosure. However, disclosing inappropriate information can increase potential risks.

For example, excessive transparency of datasets and algorithms can lead to the leakage of personal data and commercial intellectual property. The disclosure of detailed algorithmic mechanisms can also lead to the risk of targeted hacking [24]. On the other hand, an inappropriate explanation can also lead users to over-rely on the system and follow bad AI decisions [97]. Therefore, the degree of transparency of the AI system should be carefully and differently specified for the roles of public users, operators and auditors.

End-User Awareness of the Importance of AI Reliability

Beyond AI developers and vendors, end users are an important but neglected stakeholder group.

In addition to informing the general public about the core concepts of AI reliability, developers should consider how it can be presented to users so that they can gain hands-on experience with AI reliability systems. Not all aspects of reliability can be equally easily communicated to end users. For example, the impact of maintaining privacy or transparency cannot be easily demonstrated to the end user when deploying AI systems.

A deep understanding of the robustness of AI involves not only the development of better and newer AI technologies, but also requires a better understanding of the interaction between AI and human society. This

requires cooperation between different disciplines that go far beyond computer science. First, AI professionals must work closely with subject matter experts whenever AI technologies are introduced into the real world and affect people, such as in medicine, finance, transportation, and agriculture. Second, AI professionals should seek the advice of social scientists to better understand the (often unintended) social impacts of AI and work together to address them, such as the impact of AI-assisted decisions, job displacement in AI-affected sectors, and the impact use of AI systems in social networks. Third, AI professionals must carefully consider how the technology is presented to the public, as well as to multidisciplinary collaborators, and ensure that they communicate honestly and clearly the known limitations of AI systems.

Close interdisciplinary and international cooperation will serve as the basis for the rapid and stable development of reliable AI technologies, which, in turn, will benefit humanity as a whole.

References

- [1] H. Xu et al. “To be robust or to be fair: Towards fairness in adversarial training”. International Conference on Machine Learning. PMLR. 2021.
- [2] J. Hong et al. “Federated robustness propagation: Sharing adversarial robustness in federated learning”. arXiv preprint arXiv:2106.10196 (2021)
- [3] D. Tsipras et al. “Robustness May Be at Odds with Accuracy” (2019)
- [4] H. Zhang et al. “Efficient neural network robustness certification with general activation functions”. Advances in neural information processing systems (2018).
- [5] F. Bodria et al. “Benchmarking and Survey of Explanation Methods for Black Box Models”. arXiv:2102.13076 (2021).
- [6] H. Liu et al. “Trustworthy AI: A Computational Perspective”. arXiv:2107.06641 (2021).
- [7] J. M. Wing. “Trustworthy ai”. Communications of the ACM (2021).
- [8] D. Kaur et al. “Requirements for trustworthy artificial intelligence—a review”. International Conference on Network-Based Information Systems. Springer. 2020.
- [9] R. Cammarota et al. “Trustworthy AI Inference Systems: An Industry Research View”. arXiv:2008.04449 (2020).
- [10] M. Brundage et al. “Toward trustworthy AI development: mechanisms for supporting verifiable claims”. arXiv:2004.07213 (2020).
- [11] K. R. Varshney. “Trustworthy machine learning and artificial intelligence”. XRDS: Crossroads, The ACM Magazine for Students (2019).
- [12] C. S. Wickramasinghe et al. “Trustworthy AI Development Guidelines for Human System Interaction”. 2020 13th International Conference on Human System Interaction (HSI). IEEE. 2020.
- [13] A. Kumar et al. “Trustworthy AI in the Age of Pervasive Computing and Big Data”. 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE. 2020.
- [14] A. Jobin et al. “The global landscape of AI ethics guidelines”. Nature Machine Intelligence (2019).
- [15] D. Schiff et al. “AI Ethics in the Public, Private, and NGO Sectors: A Review of a Global Document Collection”. IEEE Transactions on Technology and Society (2021).
- [16] T. Hagendorff. “The ethics of AI ethics: An evaluation of guidelines”. Minds and Machines (2020).
- [17] D. Lewis et al. “An Ontology for Standardising Trustworthy AI”. Factoring Ethics in Technology, Policy Making, Regulation and AI (2021).
- [18] B. Shneiderman. “Bridging the gap between ethics and practice: Guidelines for reliable, safe, and trustworthy Human-Centered AI systems”. ACM Transactions on Interactive Intelligent Systems (TiiS) (2020).
- [19] J. Baker-Brunnbauer. “Trustworthy AI Implementation (TAII) Framework for AI Systems”. Available at SSRN 3796799 (2021).

- [20] B. Rakova et al. “Where responsible AI meets reality: Practitioner perspectives on enablers for shifting organizational practices”. *Proceedings of the ACM on Human-Computer Interaction* (2021).
- [21] D. Amodei et al. “Concrete problems in AI safety”. *arXiv:1606.06565* (2016).
- [22] A. Chakraborty et al. “Adversarial attacks and defences: A survey”. *arXiv:1810.00069* (2018).
- [23] S. H. Silva et al. “Opportunities and challenges in deep learning adversarial robustness: A survey”. *arXiv:2007.00753* (2020).
- [24] N. Akhtar et al. “Threat of adversarial attacks on deep learning in computer vision: A survey”. *Ieee Access* (2018).
- [25] X. Yuan et al. “Adversarial examples: Attacks and defenses for deep learning”. *IEEE transactions on neural networks and learning systems* (2019).
- [26] Y. Li et al. “Backdoor learning: A survey”. *arXiv:2007.08745* (2020).
- [27] Y. Vorobeychik et al. “Adversarial machine learning”. *Synthesis Lectures on Artificial Intelligence and Machine Learning* (2018).
- [28] L. Tong et al. “Improving robustness of {ML} classifiers against realizable evasion attacks using conserved features”. *28th USENIX Security Symposium (USENIX Security 19)* 2019.
- [29] T. Wu et al. “Defending against physically realizable attacks on image classification” (2020).
- [30] F. Tramèr et al. “Stealing Machine Learning Models via Prediction {APIs}”. *25th USENIX security symposium (USENIX Security 16)*. 2016.
- [31] G. R. Machado et al. “Adversarial Machine Learning in Image Classification: A Survey Toward the Defender’s Perspective”. *ACM Computing Surveys (CSUR)* (2021).
- [32] Exforsys. What is Monkey Testing. Accessed: 2021-07-09. 2011.
- [33] K. Pei et al. “Deepxplore: Automated whitebox testing of deep learning systems”. *proceedings of the 26th Symposium on Operating Systems Principles*. 2017.
- [34] L. Ma et al. “Deepgauge: Multi-granularity testing criteria for deep learning systems”. *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*. 2018.
- [35] D. Su et al. “Is Robustness the Cost of Accuracy?—A Comprehensive Study on the Robustness of 18 Deep Image Classification Models”. *Proceedings of the European Conference on Computer Vision (ECCV)*. 2018.
- [36] N. Carlini et al. “Towards evaluating the robustness of neural networks”. *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2017.
- [37] I. Goodfellow et al. “Machine learning basics”. *Deep learning* (2016).
- [38] K. Zhou et al. “Domain generalization: A survey”. *arXiv:2103.02503* (2021).
- [39] J. Wang et al. “Generalizing to Unseen Domains: A Survey on Domain Generalization” (2021).
- [40] AI HLEG. Ethics Guidelines for Trustworthy AI. Accessed: 2021-02-20. 2018
- [41] B. Goodman et al. “European Union regulations on algorithmic decision-making and a “right to explanation””. *AI magazine* (2017). [136] Google. Responsible AI with TensorFlow. Accessed: 2021-02-20. 2020.
- [42] A. B. Arrieta et al. “Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI”. *Information fusion* (2020).
- [43] R. Guidotti et al. “A survey of methods for explaining black box models”. *ACM computing surveys (CSUR)* (2018).
- [44] Z. C. Lipton. “The Mythos of Model Interpretability: In machine learning, the concept of interpretability is both important and slippery.” *Queue* (2018).
- [45] C. Molnar. *Interpretable machine learning*. Lulu. com, 2020.
- [46] A. Adadi et al. “Peeking inside the black-box: a survey on explainable artificial intelligence (XAI)”. *IEEE access* (2018).
- [47] V. Arya et al. “One explanation does not fit all: A toolkit and taxonomy of ai explainability techniques”. *arXiv:1909.03012* (2019).
- [48] B. Kim et al. “Introduction to interpretable machine learning”. *Proceedings of the CVPR 2018 Tutorial on Interpretable Machine Learning for Computer Vision, Salt Lake City, UT, USA* (2018).

- [49] T. Kulesza et al. "Tell me more? The effects of mental model soundness on personalizing an intelligent agent". Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2012.
- [50] J. R. Goodall et al. "Situ: Identifying and explaining suspicious behavior in networks". IEEE transactions on visualization and computer graphics (2018).
- [51] X. Hu et al. "Model complexity of deep learning: A survey". Knowledge and Information Systems (2021).
- [52] Y. Wang et al. "Measurement of the cognitive functional complexity of software". The Second IEEE International Conference on Cognitive Informatics, 2003. Proceedings. IEEE. 2003.
- [53] J. C. S. d. P. Leite et al. "Software transparency". Business & Information Systems Engineering (2010).
- [54] L. M. Cysneiros et al. "An Initial Analysis on How Software Transparency and Trust Influence each other." WER. Citeseer. 2009.
- [55] M. Arnold et al. "FactSheets: Increasing trust in AI services through supplier's declarations of conformity". IBM Journal of Research and Development (2019).
- [56] B. Knowles et al. "The Sanction of Authority: Promoting Public Trust in AI". Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. 2021.
- [57] AI HLEG. Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. 2020.
- [58] L. Schelenz et al. "Applying Transparency in Artificial Intelligence based Personalization Systems". arXiv e-prints (2020).
- [59] O. E. Gundersen et al. "On reproducible AI: Towards reproducible research, open science, and digital scholarship in AI publications". AI magazine (2018).
- [60] O. E. Gundersen et al. "State of the art: Reproducibility in artificial intelligence". Proceedings of the AAAI Conference on Artificial Intelligence. 2018.
- [61] R. Isdahl et al. "Out-of-the-box reproducibility: A survey of machine learning platforms". 2019 15th international conference on eScience (eScience). IEEE. 2019.
- [62] M. Zaharia et al. "Accelerating the Machine Learning Lifecycle with MLflow." IEEE Data Eng. Bull. (2018).
- [63] N. Mehrabi et al. "A survey on bias and fairness in machine learning". ACM Computing Surveys (CSUR) (2021).
- [64] S. Caton et al. "Fairness in Machine Learning: A Survey". arXiv:2010.04053 (2020).
- [65] S. Verma et al. "Fairness definitions explained". 2018 IEEE/ACM international workshop on software fairness (fairware). IEEE. 2018.
- [66] N. Grgić-Hlača et al. "Beyond distributive fairness in algorithmic decision making: Feature selection for procedurally fair learning". Proceedings of the AAAI Conference on Artificial Intelligence. 2018.
- [67] M. Bertrand et al. "Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination". American economic review (2004).
- [68] W. Xia et al. "Enabling realistic health data re-identification risk assessment through adversarial modeling". Journal of the American Medical Informatics Association (2021).
- [69] L. Rocher et al. "Estimating the success of re-identifications in incomplete datasets using generative models". Nature communications (2019).
- [70] F. Doshi-Velez et al. "Accountability of AI Under the Law: The Role of Explanation". Privacy Law Scholars Conference. (2018).
- [71] N. Diakopoulos. "Accountability in algorithmic decision making". Communications of the ACM (2016).
- [72] D. Leslie. "Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector". Available at SSRN 3403301 (2019).
- [73] I. D. Raji et al. "Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing". Proceedings of the 2020 conference on fairness, accountability, and transparency. 2020.
- [74] A. Abdallah et al. "Fraud detection system: A survey". Journal of Network and Computer Applications (2016).
- [75] S. Rabanser et al. "Failing loudly: An empirical study of methods for detecting dataset shift". Advances in Neural Information Processing Systems (2019).

- [76] I. Žliobaite et al. “An overview of concept drift applications”. Big data analysis: new algorithms for a new society (2016).
- [77] E. Samuylova. Machine Learning Monitoring: What It Is, and What We Are Missing. Accessed: 2021-05-18. 2020.
- [78] S. A. Javadi et al. “Monitoring Misuse for Accountable Artificial Intelligence as a Service”. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. 2020.
- [79] A. Abdul et al. “Trends and trajectories for explainable, accountable and intelligible systems: An hci research agenda”. Proceedings of the 2018 CHI conference on human factors in computing systems. 2018.
- [80] S. Amershi et al. “Guidelines for human-AI interaction”. Proceedings of the 2019 chi conference on human factors in computing systems. 2019.
- [81] D. S. Weld et al. “The challenge of crafting intelligible intelligence”. Communications of the ACM (2019).
- [82] A. Chatzimpampas et al. “The state of the art in enhancing trust in machine learning models with the use of visualizations”. Computer Graphics Forum. Wiley Online Library. 2020.
- [83] S. Kafle et al. “Artificial intelligence fairness in the context of accessibility research on intelligent systems for people who are deaf or hard of hearing”. ACM SIGACCESS Accessibility and Computing (2020).
- [84] C. Torres et al. “Accessibility in Chatbots: The State of the Art in Favor of Users with Visual Impairment”. International Conference on Applied Human Factors and Ergonomics. Springer. 2018.
- [85] C. Fu et al. “Monocular visual-inertial SLAM-based collision avoidance strategy for fail-safe UAV using fuzzy logic controllers”. Journal of Intelligent & Robotic Systems (2014).
- [86] M. W. Müller. “Increased autonomy for quadcopter systems: trajectory generation, fail-safe strategies and state estimation”. PhD thesis. ETH Zurich, 2016.
- [87] Q. Xu et al. “Security of Neural Networks from Hardware Perspective: A Survey and Beyond”. 2021 26th Asia and South Pacific Design Automation Conference (ASP-DAC). IEEE. 2021.
- [88] M. Sabt et al. “Trusted execution environment: what it is, and what it is not”. 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE. 2015.
- [89] S. Pinto et al. “Demystifying arm trustzone: A comprehensive survey”. ACM Computing Surveys (CSUR) (2019).
- [90] F. McKeen et al. “Intel® software guard extensions (intel® sgx) support for dynamic memory management inside an enclave”. Proceedings of the Hardware and Architectural Support for Security and Privacy 2016. 2016.
- [91] A. Asbell et al. “The role of cooperation in responsible AI development”. arXiv:1907.04534 (2019).
- [92] D. Dao. Awful AI. 2020.
- [93] I. J. Goodfellow et al. “Explaining and harnessing adversarial examples”. ICLR (Poster) 2015 (2015).
- [94] F. Tramèr et al. “Ensemble Adversarial Training: Attacks and Defenses”. International Conference on Learning Representations. 2018.
- [95] Y. Dong et al. “Evading defenses to transferable adversarial examples by translation-invariant attacks”. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2019.
- [96] A. Raghunathan et al. “Certified Defenses against Adversarial Examples”. International Conference on Learning Representations. 2018.
- [97] S. Stumpf et al. “Explanations considered harmful? user interactions with machine learning systems”. Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI). 2016.

Annex IV Artificial Intelligence as a Service

Abstract

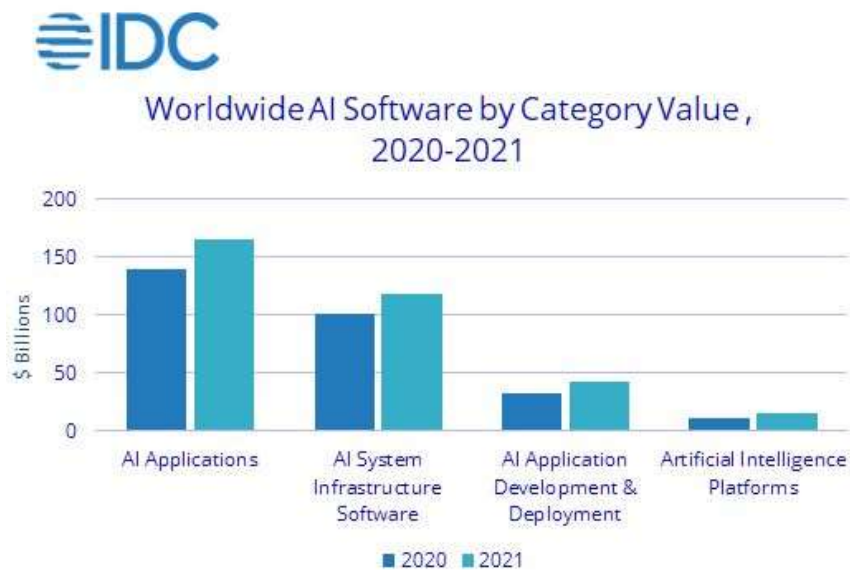
Artificial intelligence as a service is a logical and natural development of advanced artificial intelligence technology. The development of the artificial intelligence market was facilitated by a number of advantages, among which it is worth noting the technical and technological possibilities of using artificial intelligence solutions in various areas of human activity, as well as the possibility of reducing costs both for performing individual tasks and processes in complex information systems, and for introducing artificial intelligence to the end user system. It should be noted the significant impact of the COVID -19 pandemic, which forced the urgent need to transfer the spheres of human life and activity to the active use of digital technologies. Global achievements in this area were received by world-famous corporations, which had the opportunity and funds to invest in the study, development and application of artificial intelligence in healthcare, medicine, insurance, business development and others. The accumulated resources and experience have made it possible to use artificial intelligence as a service that can be used by almost anyone without high requirements for their qualifications. The requirements of different market segments and the tasks that they solve have led to the development of various artificial intelligence platforms, such as bots (chat-bots), machine learning, voice recognition, etc. This report contains the results of a study of the development of the artificial intelligence as a service market, the main advantages of its use in the state, law enforcement, social life of society, as well as the prospects for its use and development in the future.

Introduction

End users are discovering the benefits of AI across all industries as increasingly powerful AI solutions enable better decision making and increased productivity. The reality is that AI offers solutions to everything that humanity is currently facing. AI can be a source to accelerate the digital transformation process, provide cost savings at a time of staggering inflation, and support automation efforts at a time of labor shortages.

The global AI as a Service market was valued at \$2 billion in 2018 and is expected to grow at a CAGR of 34% to reach approximately \$11.5 billion by 2024 due to the increased adoption of AI to improve business-processes efficiency [1]. Organizations are using artificial intelligence to improve productivity and efficiency at a lower cost, which is expected to drive the growth of artificial intelligence as a service market over the next five years. Moreover, the growing demand to improve the user experience while reducing wait times with automated chats is likely to boost the market.

According to the next semi-annual report of IDC " Worldwide Artificial Intelligence Tracker", the global market for artificial intelligence solutions will reach almost \$450 billion in 2022 and continue to grow over the next five years. In 2021, global revenues from software, hardware and services in the field of AI amounted to \$383.3 billion, which is 20.7% more than in 2020. The largest sector was AI software in four categories: AI Application Delivery and Deployment, AI Applications, AI System Infrastructure Software, and AI Platforms. The market value of these categories exceeded \$340 billion, with AI applications accounting for almost half. AI platforms posted a 36.6% year-over-year growth.



Source: IDC 2022

Worldwide AI software by Category Value, 2020-2021

The largest sectors in the AI application category were customer relationship management (CRM) and enterprise resource management (ERM) applications, which accounted for about 16% of the category total. AI-centric applications, defined by IDC as applications where AI technologies are central and critical to their operation, accounted for 12.9% of the market in 2021, growing 29.3% year-on-year. The rest of the market is occupied by applications in which AI technologies are an integral part of certain workflows, but if these technologies were removed, the application would continue to function.

Cloud-deployed AI software is showing steady growth, and IDC predicts that in 2022, cloud deployment of newly acquired AI software will surpass on premise deployment. The data shows that in 2021, 47.3% of purchased AI software was deployed in the public cloud, up 4 percentage points from 2020 and 8.4 percentage points from 2019.

Another sector showing growth is the AI services market, which showed a 22.4% increase in total value compared to last year. IDC reports that the AI IT services category grew 21.9% year-over-year to \$18.8 billion driven by customer demand for enterprise grade AI solutions. In addition, driven by growth in demand for AI solutions for management, business processes, and HR strategy, the AI business services category grew by 24.2% in 2021.

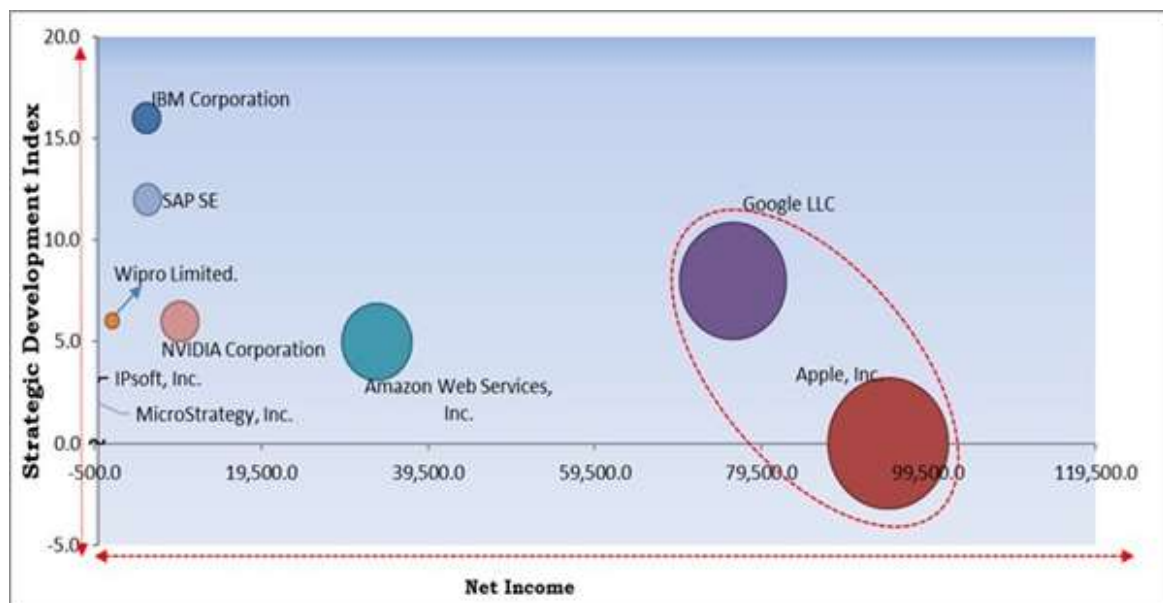
The smallest but fastest growing segment of the AI market is AI hardware. Growth of 38.9% to \$18.8 billion in 2021 was driven by efforts to create custom AI systems that can meet the growing compute and storage needs of AI models and datasets, according to IDC. AI servers and storage AI grew 39.1% and 32.9%, respectively, with \$15.6 billion in server purchases.

AI has huge commercial potential, and this is recognized by leading research companies in the IT industry. However, today's AI platforms are still cumbersome and require very large machine learning datasets, specialized applications, and highly skilled programmers. Therefore, the most powerful AI platforms are from companies that are leaders in their field. For example, International Business Machines Corp. (IBM, NYSE) has its own Watson AI platform, which is evolving towards a universal tool. Graphics processing unit (GPU) manufacturer NVIDIA Corporation (NVDA, NASDAQ) uses its hardware developments for cloud computing and machine learning technologies – the basis of AI services. Software company Microsoft (MSFT, NASDAQ) is building an AI voice assistant called Cortana that can "understand" different languages.

At first glance, these are completely different directions. However, as for other information technologies, for AI, the transition to an implementation scheme as a service is inevitable, which can be called AIaaS (Artificial Intelligence as a Service).

Analysis of the corporate artificial intelligence market

The global enterprise AI market is expected to reach \$67.2 billion by 2028, which represents a 30.9% market growth during the forecast period. AI has completely changed the way business is managed in today's business environment by integrating workflow management technologies, trend forecasting, brand purchase advertising, and other things. These are the main reasons for the growth of investment in artificial intelligence technologies. Leading market players compete with a variety of innovative offerings to stay competitive in the market. The figure below shows the percentage of revenue shared by some of the top companies in the market. Leading market players use different strategies to meet the demand from different industries. Acquisitions as well as partnerships and collaborations are key market development strategies.



The percentage of revenue shared by some of the top companies in the market

The major strategies followed by the market participants are Acquisitions. Based on the Analysis presented in the Cardinal matrix; Google LLC and Apple, Inc. are the forerunners in the Enterprise Artificial Intelligence Market. Companies such as Amazon Web Services, Inc., IBM Corporation, SAP SE are some of the key innovators in the Enterprise Artificial Intelligence Market. The market research report covers the analysis of key stake holders of the market. Key companies profiled in the report include Google LLC, Amazon Web Services, Inc., IBM Corporation, Apple, Inc., SAP SE, Wipro Limited., MicroStrategy, Inc., NVIDIA Corporation, Verint Systems, Inc., and IPsoft, Inc. .

Strategies deployed in Enterprise Artificial Intelligence Market

Partnerships, Collaborations and Agreements:

- Sep-2021: Google came into a partnership with C3 AI, a Redwood City-based enterprise artificial intelligence company. Under this partnership, C3 AI made its entire portfolio accessible on Google Cloud, which can assist companies to address various challenges and opportunities from different verticals.

- Aug-2021: Wipro teamed up with DataRobot , a leader in Augmented Intelligence. The collaboration aimed to strengthen Wipro's partner ecosystem in the dynamic Enterprise AI segment and work on its commitment to making AI accessible.
- Jul-2021: SAP extended its partnership with Google Cloud. This expanded partnership aims to assist customers to migrate critical business systems to the cloud, execute business transformations, and boost prevailing business systems with Google Cloud offerings in artificial intelligence (AI) and machine learning (ML).
- Aug-2020: SAP joined hands with Hewlett Packard Enterprise (HPE), an American multinational information technology company. This collaboration aims to provide the customer edition of SAP HANA Enterprise Cloud with HPE GreenLake , as a comprehensive managed service at the edge.

Product Launches and Product Expansions:

- Mar-2022: NVIDIA released DGX H100 Systems, World's Most Advanced Enterprise AI Infrastructure. This system is expected to empower enterprise AI factories to refine data into the most valuable resource intelligence.
- Jun-2021: NVIDIA introduced NVIDIA AI LaunchPad , a comprehensive program delivered through hybrid-cloud providers. NVIDIA AI LaunchPad is expected to put AI at the fingertips of companies everywhere with fully automated, hybrid-cloud infrastructure and software for each stage of the AI lifecycle.
- May-2021: Google unveiled Vertex AI, a new managed machine learning platform. This platform is developed to make it simpler for developers to implement and manage their AI models.
- May-2020: Amazon released Amazon Kendra, its cloud enterprise search product. This product has reinvented enterprise search by enabling customers to search across various silos of data utilizing real questions (not just keywords) and use machine learning models within the hood to know the content of documents and the relationships among them to provide the precise answers they seek.

Acquisition and Merger:

- Jul-2022: IBM took over Databand.ai, a leading provider of data observability software. This acquisition aimed to provide IBM with the most comprehensive set of observability offerings for IT across applications, data, and machine learning and is expected to continue to provide IBM's customers and partners with the technology they require to provide trustworthy data and AI at scale.
- Jul-2022: SAP completed the acquisition of Askdata , a Search-Driven Analytics Company. This acquisition aimed to strengthen SAP's capabilities to assist companies to make better-informed decisions by using AI-driven natural language searches.
- Feb-2022: IBM completed the acquisition of Neudesic , a leading US cloud services consultancy. This acquisition aimed to expand IBM's portfolio of hybrid multi-cloud services and further improve the company's hybrid cloud as well as AI strategy.
- Dec-2021: Wipro came into an agreement to acquire LeanSwift Solutions, a global leader in e-commerce and mobile solutions. This acquisition aimed to align with Wipro's strategy to invest and extend its cloud transformation business via Wipro FullStride Cloud Services. Also, the acquisition is expected to establish a robust, industry-focused Infor Practice that is expected to help Wipro win large deals in the Cloud ERP space.
- Sep-2021: SAP took over SwoopTalent , a platform that automatically connects companies' talent systems. This acquisition aimed to enable SAP to embed SwoopTalent's data and machine learning technology within SAP SuccessFactors solutions.
- Jun-2021: IBM acquired Turbonomic , an Application Resource Management (ARM) and Network Performance Management (NPM) software, provider. This acquisition aimed to add Turbonomic to IBM's portfolio.

- Dec-2020: IBM took over Instana, a German-American software firm. Through this acquisition, IBM aimed to deliver industry-leading, AI-powered automation offerings to handle the complications of modern applications that span hybrid cloud landscapes.

Depending on the size of the organization, the enterprise AI market is categorized into large enterprises and small and medium enterprises. The large enterprise segment received the largest revenue share in the enterprise AI market in 2021. The expansion of this market may be driven by factors such as growing demand for increased productivity, savings in infrastructure costs, and increased flexibility and agility by eliminating redundant jobs.

IDC regularly conducts research and provides vendor assessments of the artificial intelligence (AI) software platform market for general purpose use cases using the IDC MarketScape model. These assessments discuss both quantitative and qualitative characteristics that provide insight into software platform providers and their offerings. They cover a wide range of vendors involved in different areas of the AI software platform market and focus on detailed analysis of platform usage for a wide variety of use cases. The evaluation is based on a comprehensive and rigorous structuring of data, allowing suppliers to be evaluated against criteria and each other, and to highlight the factors that will be most influential for market success in both the short and long term.

“The adoption of AI, especially conversational AI, is past the tipping point. The rapid growth in the number of contactless interactions and the need to cut costs while improving overall service has meant that conversational is at the top of the corporate agenda,” said Dave Schubmel, vice president of research, Conversational AI and intelligent Knowledge Discovery. “Organizations are rapidly evolving and implementing conversational AI applications across all aspects of their business. This assessment will help businesses looking to implement conversational AI in the near future.”

“As organizations advance in the field of conversational AI, many are expanding the use of this technology in a variety of internal and external use cases,” said Hailey Sutherland, senior research analyst.

Conversational AI and intelligent knowledge discovery. “From assisting a distributed workforce to self-service knowledge to freeing IT help desks from black tickets and response tasks to rejecting customer calls with FAQs, organizations are realizing that conversational AI can bring value to many business areas.”

Artificial Intelligence as a Service, AlaaS

Artificial Intelligence as a Service (AlaaS) is a rapidly developing area and has become increasingly widespread in the market in recent years.

While Products as a Service, including software and infrastructure, are common in the technology industry, AlaaS as a concept is still relatively new.

AlaaS refers to the outsourcing of artificial intelligence (AI) to enable companies to explore and expand AI techniques at minimal cost. It relies on cloud computing models to leverage artificial intelligence and add significant agility to organizational operations to improve efficiency and improve productivity levels. It also helps you access AI capabilities through application programming interfaces (APIs) and tools without having to write complex codes. As a result, AlaaS is finding widespread adoption in the information and technology (IT), telecommunications, retail, manufacturing, energy and utilities, healthcare, banking, financial services, and insurance (BFSI) sectors around the world.

AI as a Service is a term used to describe a third party that provides advanced AI features to companies for a one-time payment or subscription fee.

Until recently, many companies refused to use artificial intelligence in their business, as this required their own development of systems with human qualities, such as reasoning, thinking, and learning. With AlaaS, this is more achievable than ever before, allowing companies to use artificial intelligence for things like customer service, data analytics, and factory automation.

The AI as a Service (AlaaS) market can be segmented based on technology, organization size, service type, cloud type, vertical, and region. Based on technology, the market can be divided into machine learning, natural language processing, and others. Natural language processing technology helps interpret human language and understand customer behavior, which is likely to drive growth in this segment over the forecast period. Artificial intelligence as a service finds application in various verticals, including BFSI, retail, IT and telecommunications, healthcare, government and others. The BFSI segment is likely to see widespread adoption of AlaaS before 2024 as this vertical uses AI for chatbots, fraud detection and customer recommendations. Moreover, the need for technology integration and increased operational efficiency is pushing the adoption of AlaaS in BFSI.

At the regional level, the market for AlaaS is gaining momentum and spreading to various regions around the world. The Asia Pacific industry is expected to experience the fastest growth during the forecast period. The healthcare industry in the Asia-Pacific region is growing at a rapid pace, which is due to an increase in the population and health awareness of customers. This segment creates investment opportunities in the region and is expected to drive the growth of the AI services market in the region.

Major players operating in the global AI-as-a-Service marketplace include Amazon Web Services Inc. , Google LLC , Microsoft Corp. , International business Machines (IBM) Corp. , Salesforce . com Inc. , Oracle Corporation , Fair Isaac Corporation , SAP SE , SAS Institute Inc. , Intel Corp. and others. Large companies develop advanced technologies and launch new products to remain competitive in the market. Other competitive strategies include mergers and acquisitions and new product development. For example, in 2018, Google added more AI features to its cloud to reach more customers.

Advantages and limitations

AlaaS Opportunities:

No need for complex technical skills

AlaaS is available even to those who do not have a programmer with AI skills on board - just add a code-free infrastructure layer to the game. Companies that do provide AlaaS often do not require any programming or technical skills at any stage of the setup process. In an article for Forbes Daniel Newman of Broadsuite Media Group aptly notes that “in a time of scarcity of AI experts and ever-increasing competition in the marketplace, this is a huge workaround.”

On this note, it is important to highlight that while some AlaaS solutions do not require any coding skills, the level of implementation complexity varies greatly when we enter the world of legacy software.

Developed infrastructure – and quickly

Before AlaaS, running successful AI and machine learning models required powerful and fast GPUs. Most SMBs do not have the resources and time to develop software in-house.

There are a few rules of thumb in the AI world - one of them is that your model will only perform well on a task if the data it receives is of good quality. Customizability AlaaS will provide the ability to build a specific task-based model based on a wealth of data that is already in use by most organizations.

“By the end of 2023, the global AlaaS market will be valued at just under \$11 billion, with a CAGR of 2017-2023 hovering around the 49% mark.” - Hussein Fakhruddin , CEO of Teksmobile

Transparency

AlaaS not only gives you access to AI while reducing non-value-adding labor, but also provides a significant degree of transparency. AlaaS allows you to pay per use – machine learning requires a lot of computing power, but most pricing models are usage oriented.

Additionally, some platforms allow the user a little more control over the AI automation.

The way to do this is to add the person to the loop as an option. HITL is a continuous feedback loop in which process owners provide feedback to the AI in extreme cases. This function aims to achieve what neither man nor machine can achieve on their own.

Ease of use

Let's be honest: most platforms as a service are not as user-friendly as we would like them to be. While many AI options are open source, meaning they are free to download, modify, and use, they can be difficult to install and develop. AlaaS, in most cases, is completely ready for use. Process owners can use AI software without any formal training.

Comprehensive machine learning services include both off-the-shelf and user-created models, as well as drag-and-drop interfaces to simplify. Cool in this? Get your machine learning project up and running in hours without the help of engineers.

Scalability

Have you ever heard of an organization that gets fewer emails as it grows? Yes, we do too.

AlaaS is built to scale. If you have trained your model to categorize your information based on urgency or email sentiment and direct the right emails to the right person, you are already ahead of the game. AlaaS is ideal for performing tasks that require a certain level of cognitive judgment, but the task itself adds no value.

Price

Sophisticated software is expensive, while subscription allows you to recoup costs over a long period of time, making the products more affordable for small businesses. In addition, many companies do not have the resources to develop software in-house and may consider licensing off-the-shelf software as a cheaper option.

Relevance.

Unlike the annual purchase of the latest iteration of expensive software, the service involves constant access to its latest version. Since many AI platforms are in a state of constant development and adjustment, constant updating is a big advantage.

Infrastructure.

AlaaS providers are engaged in data center maintenance and processing, removing these responsibilities from the client.

Development.

A constant flow of customer payments allows the service provider to direct more funds for development, add new features, fix bugs and continue to improve the product.

AlaaS Limitations:

Closed source code.

Supporters of the Open Source is often frustrated that AlaaS products are mostly closed source.

Customer does not own it.

Companies have been known to unilaterally terminate their AI services, leaving their customers looking for alternatives. In addition, the client may find that the product does not fully meet their needs, and instead want to develop in a different direction. Hence: owning a product has its advantages;

Price.

Over time, the cost of the service pays off many times over, and it would be better to pay a lump sum up front. In many cases, buying isn't even an option—a clear indication that service providers see the lease as more profitable. It's an impressive feat when a machine can mimic human intelligence. This can be very

expensive and requires a lot of time and resources. AI is very expensive because it requires the latest hardware and software to stay up to date and qualify. A significant disadvantage is the inability of AI to learn to think outside the box creatively. Using preloaded data and previous experience, the AI can learn over time, however it cannot use a new method. These reports contain only information that has already been sent to the bot.

There is not always the best solution.

Most people prefer to deal with their own kind, but, oddly enough, there are those who do not mind communicating with chatbots. In other words, chatbots can be disliked;

Failures with AI.

Companies rushing to adopt advanced technologies are often disappointed. In 2020, Google 's medical AI made headlines for failing to transfer success from the lab to the real world, causing retinal image analysis to take longer than expected. IBM Watson made similar mistakes, including when implemented in hospitals.

Types of AI platforms as a service and the problems they solve

Bots

At present, whether the Internet is being searched for information, from government websites to clothing stores, it is likely that the resource will use a bot, especially their most common type, the chatbot.

They use natural language processing (NLP) algorithms to simulate natural conversations between people. These types of bots are mainly used for customer service and provide relevant answers to the most frequently asked customer questions. Because they answer 24/7, they save time and resources by allowing employees to focus their time on more complex tasks. In fact, one of the fastest growing package delivery companies in Europe, InPost, recently reported that they automate up to 92% of the millions of customer conversations they have every year with a chatbot.

API

An API (Application Programming Interface) is software "intermediary" that allows two applications to communicate with each other. An example of this would be a third-party airline booking website such as Expedia , CheapOair , or kayak , which pull information from a set of airline databases to present all their offers in one place in a human-readable way. APIs are critical for connecting applications to each other. Common API applications also include:

- Natural language processing (e.g. sentiment or urgency analysis)
- Computer vision
- Conversational AI

Machine learning

Machine learning (ML) is used by companies to analyze and find patterns in their data. As a result, he makes predictions that they were not specifically taught, learning as the process develops. This method of data analysis is designed to operate with little or no human intervention. In AlaaS, companies can manage machine learning without having any special technical knowledge - there are many solutions, from pre-trained models to creating a model to perform a custom task (just remember the rule of thumb!).

Data marking

Data labeling is essentially annotating large amounts of data so that it can be organized efficiently. It has a wide range of use cases - such as ensuring data quality, classifying it by size, and further training your AI, just to name a few. In the latter case, the person in the loop (which we mentioned earlier in this post) is used to label the data so it can be easily assessed by AI in the future.

Data classification

Data classification is when data is tagged into one or more categories. Classifications typically include content-based, context-based, and user-based. With the use of artificial intelligence, data can be classified on a larger scale, provided that the data classification scheme and criteria are clearly defined. Here is a great visual example of how a business can use data classification:

The Fields of AlaaS Application

The enterprise artificial intelligence (AI) market has expanded as a result of the growing demand for innovative and advanced enterprise AI products in a number of industries, including retail, healthcare and education. Media and advertising, retail, finance, healthcare, agriculture, education, oil and gas, automotive and transportation, legal and other industries are just some of the many areas where AI is being used. Thanks to advances such as self-driving cars, accurate weather forecasts, space exploration, etc., the AI market has become global. With its ability to evaluate vast amounts of genomic data and provide more accurate disease prevention and treatment, AI is also expected to have an impact on health care breakthroughs.

AI is also being used to analyze big data sets and make predictions, optimize information storage, or even detect fraudulent activities. Amazon 's Personal Recommendation System - AI powered by machine learning - is now available as a licensed service to other retail chains, video streaming platforms, and even the financial industry. Google 's AI services range from natural language processing, handwriting recognition to captioning and real-time translation. Watson 's pioneering AI , developed by IBM , is currently being used to fight financial crime, targeted advertising based on real-time weather analysis, and data analysis to help hospitals make treatment decisions.

Artificial intelligence plays an important role in M2M (machine-to-machine) communication as companies rapidly innovate to compete in high-tech markets.

According to Future Market Insights analysts, the machine-to-machine (M2M) market will be valued at \$376 billion by 2032. Its total volume for the period from 2016 to 2021 will be amounted to 336 billion dollars. As you can see, the market is growing rapidly. And as the market grows, so do M2M networks as companies look to the future.

M2M describes the interaction between multiple machines or pieces of equipment without human intervention. By remaining simultaneously connected to the Internet and to each other, M2M systems allow countless devices to "talk" to each other, exchanging data to streamline daily life and business processes.

M2M is closely related to the concept of the Internet of Things (IoT), which describes a network of devices connected to the Internet and to each other.

In the world of M2M, artificial intelligence essentially improves the efficiency of processes and data through automation. The AI is particularly good at top-level repetitive tasks. This can be useful for managing the M2M data you receive through methods such as sensor fusion. However, regardless of whether the M2M process is connected to the Internet, AI machines can use sensor data to automate business processes and improve the real-time experience. However, even with AI, it's useful to have a human on hand to troubleshoot any issues.

Smart Company Engines specializes in the development and delivery of complex industrial-level software solutions for automating recognition and data entry from documents in a video stream, in photographs and scans.

In 2020 Smart specialists Engines has developed its own neural network architectures, the use of which in X-ray computed tomography allows to reduce the required dose of radiation to patients. Scientists Smart Engines has created algorithms that allow you to reconstruct the image immediately during the process of tomographic imaging and stop the study when a result of sufficient quality is reached. The decision will be relevant, in particular, for examinations of patients with COVID-19.

In 2021, Smart Engines released the first version of the Smart product Tomo Engine, which contains all the necessary API documentation for loading data, performing tomographic reconstruction, and saving results.

Perspective of AiaaS

There is currently an increase in the use of AI technology in many organizations for their applications, business, analytics and services. This, along with the growing demand for cloud-based machine learning (ML) to reduce operating costs and increase profits, represents one of the key factors driving the market. Moreover, the governments of a number of countries are actively investing in the development of infrastructure based on AI. This, coupled with the growing trend of multi-cloud management strategies around the world, is driving the growth of the market. In addition, the increasing use of artificial intelligence technologies in the BFSI industry to improve consumer experience has a positive effect on the market. In addition, the growing need for predictive and intelligent business process automation to grow the service and product portfolio offers lucrative growth opportunities for industry investors. In addition, the increased use of AI technology in various Internet of Things (IoT) devices by electronics manufacturers for natural language generation, virtual agents, and speech recognition is predicted to drive market growth in the coming years.

Over time, the accuracy of AI varieties improves through machine learning. Some have become so complex, like the GPT-3 language model, produce entire volumes of text that are virtually indistinguishable from a genuine human source.

Microsoft has even used GPT-3 to translate spoken language into working computer code, potentially opening up new horizons in software writing in the future and giving coding newbies a chance. Microsoft is also partnering with NVIDIA to create a new natural language generation model that is three times more powerful than GPT-3. Improvements in language recognition and generation have clear benefits for the future development of chatbots, home assistants, and document generation.

Industrial giant Siemens announced the integration of Google's AIaaS solutions to optimize, analyze data and predict, for example, the wear rate of factory equipment. This will help reduce maintenance costs, improve inspection scheduling, and prevent unexpected equipment breakdowns.

AIaaS is a rapidly growing field, and there will be many more niches to fill in the coming years.

The pandemic has accelerated the adoption of digital technologies in almost all industries, and this is affecting IT and business strategy, writes on the InformationWeek portal Amit Patel, Senior Vice President Consulting Solutions.

As organizations manage the risks and vulnerabilities that result from digital transformation, cybersecurity must continue to improve to keep pace with the ever-evolving and increasingly sophisticated cybercrime practices. Artificial intelligence, machine learning, and process automation (RPA) can help detect malware and ransomware. For example, advanced algorithms help to tighten security, especially when combined with automation tools.

As a component of the aforementioned cybersecurity, AI has a much broader and deeper impact on other areas of business, and is projected to exceed \$126 billion in market size by 2025. At a high level, AI-based business tools allow organizations to predict more accurately, which in turn helps improve operations, more accurately estimate future sales and earnings, and more quickly recognize market trends.

References

- [1] Research and Markets, "Global Artificial Intelligence as a Service Market by Technology, By Organization Size, By Service Type (Services & Software Tools), By Type of Cloud, By Vertical, By Region, Competition, Forecast & Opportunities, 2024", Research and Markets, [Online]. Available: <https://www.researchandmarkets.com/reports/5585321/global-artificial-intelligence-as-a-service-market-by#rela4-4833051>
- [2] Research and Markets, "Global Enterprise Artificial Intelligence Market Size, Share & Industry Trends Analysis Report By Vertical, By Deployment Type (Cloud and On-premise), By Organization Size, By Technology, By Regional Outlook and Forecast, 2022 – 2028", Research and Markets, [Online].

Available:

<https://www.researchandmarkets.com/reports/5645560/global-enterprise-artificial-intelligence-market#rela2-4833051>

- [3] Research and Markets, “Artificial Intelligence-as-a-Service Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2022-2027”, Research and Markets, [Online].

Available:

<https://www.researchandmarkets.com/reports/5647631/artificial-intelligence-as-a-service-market#rela1-4833051>

- [4] Research and Markets, “Artificial Intelligence as a Service Market, By Service Type (Software Tools, Services), Technology, Organizations Size, Software Tool, Vertical, Region (North America, Europe, Asia Pacific, Rest of the World) - Global Forecast to 2028”, Research and Markets, [Online].

Available:

<https://www.researchandmarkets.com/reports/5616532/artificial-intelligence-as-a-service-market-by#rela0-4833051>

- [5] Raj Bala, Bob Gill, and 3 more, “Magic Quadrant for Cloud Infrastructure and Platform Services”, [Online]. Available:

<https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb>

- [6] Forester, “Three Strategic Consideration For AI Success”, Forester Analytics Business Technographics. Data and Analytics Survey, 2021. [Online]. Available: <https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb>

Annex V P300 technology for HUMINT

Brain fingerprinting is a controversial investigative technique that measures whether specific information is stored in a subject's brain. The technique consists of measuring, through electroencephalography (EEG), a person's electrical brainwave response to words, phrases, or pictures that are presented on a computer screen.

Brain fingerprinting was invented by Lawrence Farwell in the 1990s. Its theory explains that the suspect's reaction to the details of an event or activity will reflect if the suspect had prior knowledge of the event or activity [1]. Farwell's brain fingerprinting originally used the well-known P300 brain response to detect the brain's recognition of the known information [1] [2].

Later Farwell discovered the "Memory and Encoding Related Multifaceted Electroencephalographic Response" (MERMER), which includes the P300 and additional features and is reported to provide a higher level of accuracy than the P300 alone [3] [4] [5]. Brain fingerprinting technology has been used to help solve some criminal cases in the United States (US). The technique has also been used by police in India and Singapore, and recently in the United Arab Emirates (UAE). This report examines and explores brain fingerprint technology for deception detection: how it works, and the methodology used. This report also highlights its potential advantages and limitations for operational use within the intelligence gathering cycle and law enforcement criminal justice investigations.

Introduction

Interviews and interrogations are key elements of the intelligence and evidence gathering process for intelligence and law enforcement enforcement agencies. The main goal of gathering criminal intelligence and evidence from human sources is to elicit truthful and operationally useful information from another person. Different kinds of instrumentation, techniques, and procedures exist to assess the truthfulness of individuals to unveil concealed information. These approaches can be broadly divided into behavioural and technology-based categories [6]. A typical example of the technological-based approach is the polygraph examination (lie-detector), while the cognitive interview is a good example of the behavioural approach, being a method initiated within child and clinical psychology which has migrated to the intelligence and law enforcement domains which seeks to improve the subject's memory retrieval processes. [7]. In this paper, we focus on technological based approaches, specifically on the so called 'brain fingerprinting' technology, a controversial technique used to determine whether specific information is stored in an individual's brain. The technique can be applied in criminal and intelligence investigations to detect concealed information. However, brain finger printing is only valid in situations where investigators have sufficient specific information about an event or activity that would be known only to the perpetrator and the investigator.

The brain fingerprinting technique uses electroencephalography (EEG) to detect the increased rate of brainwaves. Typically, the process consists of attaching electrodes to a suspect's head and showing them pictures. When the suspect sees an image that they have seen before, a particular electrical signal (P300-MERMER) is amplified in the brain. The brain responses are read by EEG electrodes and represented on a computer screen. The results are submitted to prosecutors, but it is left to the judge to determine if the suspect is guilty or not. Nothing is done without the suspect's consent.

Unlike the polygraph, the brain responses measured by brain fingerprinting technology is not influenced by emotions such as fear, stress, or anxiety. A conventional polygraph test relies on flashes of sweat from the autonomous nervous response, a physiological panic brought on by lying. Instead, the brain fingerprinting

response is entirely confined to the brain, making it significantly harder to deceive the test; the usual polygraph tricks won't work to deceive examination, and the system is much more resistant to adversaries [8]. However, unlike polygraph testing, brain fingerprinting does not attempt to determine whether the subject is lying or is telling the truth. Rather, it measures the subject's brain response to relevant words, phrases, or pictures to detect if the relevant information is stored in the subject's brain or not. It is left to the judge or jury to determine if the subject is guilty or innocent. For this reason, brain fingerprinting is used today only as a tool which supports and informs law enforcement agency investigations and intelligence agency operations.

History

Invented by Dr. Lawrence A. Farwell in 1990, brain fingerprinting technology was used for the first time in 1999 to help solve a 15-year-old murder case in the US. A woodcutter named James B. Grinder confessed the murder of 25-year-old woman named Julie Helton. During the 15-year criminal procedure, Grinder gave several different testimonies, recanting and contradicting himself over and over. The testimonies were invariably contradictory to the available material evidence. Moreover, the DNA test did not bring favourable results since the blood samples taken at the crime scene were old. After approximately 10,000 hours of unsuccessful investigation, the local police decided to turn to brain fingerprinting testing to decide if Grinder had committed the crime. During the test analysis, Farwell showed Grinder specific details of the crime, and he concluded that all the critical information was stored in Grinder's brain (Figure1). Then, following the principles of the method, the conclusion was that Grinder did commit the offence since his brain had enhanced MERMER response to all relevant information [9].

Afterwards, Farwell tested the device on two other murder cases before founding his own company, the "Brainwave Sciences". In 2013, the company made its first sale to Singapore's police force. To date, brain fingerprinting is considered a technique of proven accuracy for US government tests, and it has been ruled as admissible in one US court as scientific evidence. The Brainwave Sciences device has been tested by several US federal government agencies, which found it to be almost 100% accurate. The technique has also been used in Indian courts and, recently, has been used to solve two murders in the UAE [8]. In the UAE, Dubai Police carried out a year of trials on the "Memory Print" before putting it to use to aid investigations. However, an experimental study about the device is still under way in collaboration with Dubai Police Academy to conduct more systematic investigations into how it works and its level of efficacy. [10]



Figure 1 - Dr. Larry Farwell conducts a brain fingerprinting test on serial killer J.B. Grinder, a suspect in the murder of Julie Helton. The test showed that Grinder's brain contained a record of certain salient features of the crime. He pled guilty and was sentenced to life in prison

P300 response

The basis of brain fingerprint technology is the P300 (or P3) brain wave response. When a stimulus (image, written text, etc.) is presented to an individual, a brief electrical transient occurs after a short and characteristic time delay. This transient evoked by a particular stimulus is referred to as the event-related-potential (ERP). A given ERP is conventionally labelled as positive-going (P) or negative-going (N) along with the approximate delay (in milliseconds) after stimulus onset at which the transient typically occurs (e.g., P300 or N400).

The most studied ERP is known as the P300. Commonly referred as the ‘oddball’ response, the P300 is a large positive deflection in the EEG response that follows the presentation of a stimulus, typically between 250 and 350ms. Figure 2 shown below provides an example of an ERP signal (P300). The signal is typically measured most strongly by the electrodes covering the parietal lobe. The size of the P300 can be influenced by a variety of factors, including stimulus relevance to a task, cognitive load, probability of occurrence, and others [11] [12]. But the P300 is most consistently elicited by an oddball stimulus: a rarely presented stimulus that qualitatively differs from other recent stimuli [2]. The response is thought to reflect the neural activity generated when a mental expectation or prediction is violated, or a significant change is registered by the brain. If attention is kept high during the exposure to stimuli that are irrelevant, unfamiliar, or insignificant to an individual, the rare stimulus that is relevant, familiar, or salient to an individual can be expected to elicit a P300 response.

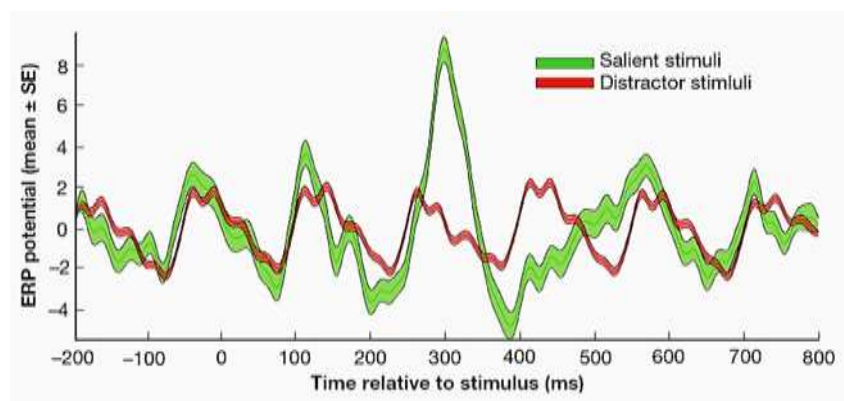


Figure 2 - Example of ERP signal

P300 is considered to be an endogenous potential as its occurrence links not to the physical attributes of a stimulus but to a person’s reaction to the stimulus.

Since the initial discovery of the ERP component, research has shown that the P300 is not a unitary phenomenon but can be distinguish between two subcomponents of the P300: P3a and P3b. The P3a is a positive-going scalp-recorded brain potential that has a maximum amplitude over frontal/central electrode sites with a peak latency falling in the range of 250-280ms [13]. The P3a has been associated with brain activity related to engagement of attention, especially orienting and involuntary shifts changes in the environment, and the processing of novelty. The P3b is a positive-going ERP amplitude peaking at around 300ms, though the peak varies in latency from 250-500ms or later. The P3b has been used as a tool to study cognitive processes, especially psychology research on information processing. Improbable events will elicit a P3b, and the less probable the event, the larger the P3b [14]. However, in order to elicit P3b, the improbable

event must be related to the task at hand in some way (e.g., the improbable event could be an infrequent target letter in a stream of letters, to which a subject might respond with a button press).

Brain fingerprinting technique relies on reproducible elicitation of the P300 wave, central to the idea of a Memory and Encoding Related Multifaced Electroencephalographic Response (MERMER), developed by Dr. Lawrence Farwell. While researching the P300, Dr. Farwell created a detailed test that not only included the P300, but also observes the stimulus response up to 800ms after the stimulus. He calls this response MERMER (Memory and Encoding Related Multifaced Electroencephalographic Response). This P300 has a peak latency of approximately 300 ms to 800 ms. The MERMER includes the P300 and, also, includes an electrically negative component with an onset latency of approximately 800-1200 ms. The MERMER response is not present in subjects who lack specific knowledge about a word, phrase, or picture presented; for this reason, MERMER response is considered to be linked to familiarity and recognition, providing positive potential use within intelligence operations and criminal investigations for detecting concealed information.

The technique

The procedure used shares similarities with the Guilty Knowledge Test (also known as Concealed Information Test) used also in polygraph examinations: a sequence of words, phrases, or pictures is presented on a video monitor to the subject for a fraction of a second each. The subject wears a special headband with electronic sensors that measures EEG signals from several locations on the scalp. The entire Brain Fingerprinting system is under computer control, including presentation of the stimuli, recording of electrical activity. A mathematical data analyses algorithm that compares the response of stimuli produces two possible outcomes: ‘information absent’ (the details of the crime are not stored in the brain of the suspect) or ‘information present’ (the details of the crime are stored in the brain of the suspect) [15]. Three types of stimuli are presented and represented by different coloured lines [16]:

- 1) **TARGET:** the target stimuli (red line) is chosen to be relevant information to the tested subject. The target stimuli is information the suspect is expected to know.
- 2) **IRRELEVANT:** these (green line) have no relation to the situation under investigation. Irrelevant stimuli is information related to the crime that the suspect claims to have no knowledge of.
- 3) **PROBES:** probes (blue line) are the stimuli that are relevant to the situation under investigation. For example, this is information of the crime that only the suspect would know.

Target stimuli are used to establish a baseline brain response information that is significant to the subject being tested. The subject is instructed to press one button for Targets, and another button for all other stimuli. The irrelevant stimuli does not elicit a MERMER response, and so does not establish a baseline brain response for information that is insignificant to the subject in that context. The Probe stimuli will elicit a MERMER, signifying that the subject has responded to stimuli showing it to be significant. If the subject is lacking this information in their brain, the response to the Probe stimuli will be indistinguishable from the irrelevant stimuli (Figure 3). This response does not elicit a MERMER, indicating that the information is absent from their mind.

A subject lacking specific information relevant to the situation under investigation recognizes only two types of stimuli: targets and irrelevant. Instead, a subject with specific information relevant to the situation under investigation, recognizes all three types of stimuli: targets, irrelevant, and probes.

Before the test, the scientist also makes sure that the subject does not know the probes for any reason unrelated to the crime, and the subject denies knowing the probes. The subject is told why the probes are significant but is not told which items are the probes and which are irrelevant [16].

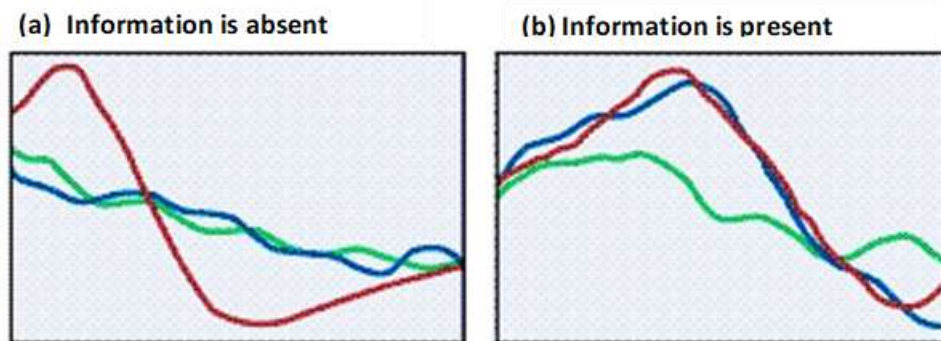


Figure 3 (a) Information is absent: because the blue (PROBE) and green lines (IRRELEVANT) are closely correlated, subject does not have critical knowledge of information. (b) Information is present: because the blue (PROBE) and red lines (TARGET) are closely correlated, subject has critical knowledge of information.

The four phases of Farwell brain fingerprinting

The application of Brain Fingerprinting testing in criminal case consists of four phases: investigation, interview, scientific testing, and adjudication. The first phase is undertaken by an investigator, the second by an interviewer, who may be an investigator or a scientist, the third by a scientist, and the fourth by a judge and jury [17].

1. **Investigation:** the first phase in applying brain fingerprinting testing is an investigation of the crime to identify details of the crime that would be known only to the perpetrator. Before a brain fingerprinting test can be applied, an investigation must be undertaken to collect information that can be used in the test. The role of the investigation is to find specific information that will be useful in a Brain Fingerprinting test.
2. **Interview of the subject:** Once evidence has been collected through investigation, it can in some cases be very useful to obtain the suspect's account of events in question. The suspect is asked if they would have any legitimate reason for knowing any of the information that is contained in the potential probe stimuli. This information is described without revealing which stimuli are probes and which are irrelevant.
3. **Scientific Testing with Brain Fingerprinting:** Brain fingerprinting test determines scientifically whether or not specific information is stored in the suspect's brain. The method used is the same described in the previous section. The output of this procedure is a determination of "information present" or "information absent" for specific probe stimuli. The determination is made according to an algorithm which computes statistical confidence for that determination.
4. **Adjudication of Guilt or Innocence:** the final step is the adjudication of guilt or innocence. This phase is conducted entirely outside the domain of science. The decision is the exclusive domain of the judge and jury; it is not the domain of the investigator, scientist, or the computer. Science provides the evidence, but a judge and jury must evaluate the evidence and decide the verdict.

Applications of brain fingerprinting

National Security, Counter terrorism

Brain fingerprinting testing provides an accurate, economical, and timely solution to the problem of the fight against terrorism. This technique can determine with an extremely high degree of accuracy those who are involved in terrorist activity and those who are not [16]. Specifically, brain fingerprinting can help to address the following critical issues:

- Aid in determining who has participated in terrorist acts, directly or indirectly.
- Aid in identifying trained terrorists with the potential to commit future terrorists' acts, even if they are in a 'sleeper' cell and have not been active for some time.
- Help to identify people who have knowledge in banking, finance, or communications and who are associated with terrorist groups and related attack planning or other supportive activities.
- Help to determine if an individual has a leadership role within a terrorist organization.

In a terrorist investigation, especially a long protracted investigation that remains covert and seeks to disrupt and prevent a terrorist attack, there may be an absence of reliable forensic evidence such as fingerprints or DNA. However, the brain of the perpetrator is always present, planning, preparing, executing, and recording the crime together with the intention to commit the crime [16]. Therefore, the terrorist plotter has knowledge that an innocent person does not have. A brain fingerprinting test can determine those who are involved with terrorist activity and those who are not engaged in the commission, preparation or instigation of an act of terrorism.

The technique has already been tested in the counter-terrorism field. In a study with the FBI, Dr. Farwell and Federal Bureau of Investigation (FBI) scientist Drew Richardson, former chief of the FBI's chem-bio-nuclear counter-terrorism unit, used brain fingerprinting to demonstrate that test subjects from specific groups could be identified by detecting specific knowledge which would only be known to members of those groups [18] [19]. A group of 17 FBI agents and 4 non-agents were tested. The probe stimuli contained information that only FBI agents could know. Brain fingerprinting was able to correctly distinguish the FBI agents from the non-agents.

Criminal justice

The overarching aim of any criminal justice system is to determine who has committed a crime, bringing them to justice in a court of law. The main difference between a guilty and an innocent suspect is that the perpetrator of a crime has a record of the crime stored in their brain, instead the innocent suspect does not. Fingerprinting and DNA evidence are available in only 1% of major crimes [30]. Brain fingerprinting provides the judge and jury with valid scientific evidence to help inform them make their decisions. The potential impact upon any criminal justice system approving the admissibility of brain fingerprinting evidence will be profound. Brain fingerprinting technology could dramatically reduce the costs related to investigating and prosecuting innocent people, and allow law enforcement professionals to concentrate on suspects who have verifiable, detailed knowledge of the crime under investigation. The application of brain fingerprinting within the criminal justice process has positive potential to reduce miscarriages of justice. Moreover, for investigators and intelligence gatherers progressing prosecution cases, it has the potential to better direct the strategy and focus of an investigation, thereby saving valuable time and resource, increasing the expedience and efficacy of an investigation.

Other Applications

Brain fingerprinting has potential application in other fields. In medicine, the technology can be used to measure how memory and cognitive functioning of Alzheimer sufferers are affected by medications. Medical professional specialists can use it to measure how quickly information is disappearing from the brain and if the drugs they are taking are slowing down the process.

Another application could be in the field of advertising. Most advertising programs are evaluated subjectively using focus groups. Brain fingerprinting laboratories could be used to help determine the efficacy of campaigns. For example, in a branding campaign it could determine whether people remember the brand, the product, etc., and measure the comparative effectiveness of multiple media types. In the insurance industry as another commercial example, brain fingerprinting would be able to reduce the incidence of insurance fraud by determining if an individual has knowledge of fraudulent or criminal acts; or by determining if an individual has specific knowledge related to computer crimes.

Advantages and limitations

In summary, the main advantages of brain fingerprinting respect to other investigative techniques (e.g., polygraph) include the following:

- The technique is based on EEG signals: the system does not require the tester to issue a verbal response to questions or stimuli
- It uses cognitive brain responses, and it does not depend on the emotions of the subject, nor is affected by emotional responses. Instead, polygraph (that is a lie-detector) is influenced by emotion-based signals.
- It can identify criminals quickly and scientifically. It has an accuracy of almost 100%, as claimed by Farwell.
- The use of this technique reduces expenditure of money, time and other resources.

However, it also presents several disadvantages:

- Brain fingerprinting can detect what information is stored in the subject's brain, but it does not detect how that information got there, be it a witness or a perpetrator.
- Brain fingerprinting detects only information, not the intent. The fact that the suspect knows the uncontested facts of the circumstance does not tell us which party's version of the intent is correct [20].
- If the investigators have no idea what crime or act the individual may have committed, there is no way to structure appropriate stimuli to detect the tell-tale knowledge that would result from committing the crime. Brain fingerprinting can, however, be used for specific screening, when investigators have some idea what they are looking for. For example, the technique can be used to detect whether a person has knowledge that would identify him as an FBI agent, an Al-Qaeda-trained terrorist, a member of a criminal organization or terrorist cell, or a bomb maker [19].
- Brain fingerprinting is not a lie-detector. It simply detects information. No questions are asked or answered during brain fingerprinting test. Then, the outcome of the test is unaffected by whether he has lied or told the truth at any other time [16].

- Brain fingerprinting depends on the memory of the subjects. How does the test hold up on neurologically atypical suspects, like psychopaths or the mentally ill? It is not clear how scientists can control those factors, and they could leave a dangerous loophole if the method is more widely adopted [8].
- Brain fingerprinting is not a substitute for effective investigation on the part of the investigator or for common sense and good judgment on the part of investigator or for common sense and good judgment on the part of the judge and jury [16].
- Like all forensic science techniques (such as DNA test), brain fingerprinting depends on the evidence-gathering process which lies outside the realm of science. Brain fingerprinting tests determine only whether the information stored in the suspect's brain matches the information contained in the probe stimuli [16].

Next steps

The investigation to examine and explore the potential of P300-related cognitive technologies for deception detection by government agencies across EU Member States has identified the potential positive applications and operational challenges and considerations for HUMINT and other intelligence disciplines, providing a richer picture of the P300 landscape. It is evident from these further investigations – despite the challenges and limitations noted – that P300 provides a real and unique opportunity to profoundly impact upon intelligence operations and law enforcement agency investigations.

Although P300 techniques, tools, technologies and tactics are not commonly used or applied in the EU at this time, there remains the potential for significant positive impact upon and within member states' criminal justice systems. This further investigation serves to dispel the myth that brain-fingerprinting is pseudo-science or science fiction but is science fact, with a growing body of evidence from real world practice that adds value to the intelligence gathering phases and has potential for further investigative application. With any cutting-edge technology or technological advancement it is common to dismiss their future potential but the purpose of NOTIONES must be to prepare security and intelligence agencies to meet the future threats and challenges that lie ahead, including those recently identified by Europol in their report: Policing the metaverse: What law enforcement agencies needs to know¹⁰. The ethos of NOTIONES is not only to support the needs of the security and intelligence services for future security research programming but also to monitor technologies and to define the requirements and recommendations for their industrialization to provide a great advantage to practitioners in the fields of intelligence and security. It is therefore recommended that:

Brain-fingerprinting and related P300 tools, tactics, techniques and technologies be subject to further monitoring and analysis conducted with end-user practitioners to scope the potential operational opportunities, applications and impacts upon intelligence operations and law enforcement investigations. This scoping activity will inform a roadmap of research requirements proving an evidence base to support for future security research programming.

References

¹⁰ <https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>

- [1] F. L.A. e D. E., «The Truth Will Out: Interrogative Polygraphy ("Lie Detection") With Event-Related Brain Potentials,» *Psychophysiol.*, n. 28, pp. 531-547., 1991.
- [2] F. LA, «Method and Apparatus for Truth Detection.,» in U.S. Patent, 1995a.
- [3] F. LA, «Method for Electroencephalographic Information Detection.,» U.S. Patent, 1995b.
- [4] F. LA e S. SS, «Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal,» *J. of Forensic Sciences*, vol. 1, n. 4, pp. 135-143, 2001.
- [5] F. LA, «Method and Apparatus for Multifaceted Electroencephalographic Response Analysis (MERA),» U.S. Patent, 1994.
- [6] K. Heckman e M. Happel, «Mechanical Detection Deception: A short Review,» in *Educing Information: Interrogation: Science and Art*, Washington, DC: R. Swenson, 2006, pp. 63-94.
- [7] M. D. Happel, J. A. Spitaletta, E. A. Pohlmeier, G. M. Hwang, C. A. S. A. M. Greenberg e M. Wolmetz, «National Security and the Assessment of Individual Credibility: Current Challenges, Future Opportunities,» *Jhons Hopkins APL Technical Digest*, vol. 33, n. 4, 2017.
- [8] R. Brandom, «Is 'brain fingerprinting' a breakthrough or a sham ? The controversial method claims to look inside a suspect's brain to see the details of a crime- but hwo much can it see ?,» *The Verge*, 2015.
- [9] Budaházi e Árpád, «Brain Fingerprinting as lie detection technique,» Budapest, Hungary.
- [10] S. A. Amir, «Brain fingerprinting: Dubai Police give exclusive glimpse at crime-fighting technology. A guilty suspect's brainwaves can give them away if presented with an image, scene or weapon they have seen before,» *The National*, May 2021.
- [11] I. Berlad e H. and Pratt, «"P300 in Response to the Subject's Own Name",» *Electroencephalogr. Clin. Neurophysiol*, vol. 96, n. 5, p. 472–474, 1995.
- [12] R. JP, B. JR, K. MJ e S. KM, «Subjective and objective probability effects on P300 amplitude revisited,» *Psychophysiology*, vol. 42, n. 3, pp. 356-359, 2005.
- [13] M. D. Comerchero e J. Polich, «P3a and P3b from typical auditory and visual stimuli" (PDF).,» *Clinical Neurophysiology.* , vol. 110, n. 1, p. 24–30., 1999.
- [14] P. J., «Updating P300: An integrative theory of P3a and P3b,» *Clinical Neurophysiology*, vol. 118, n. 10, pp. 2128-2148, 2007.
- [15] L. Farwell, «Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials,» *Cognitive Neurodynamics*, n. 6, 2012.
- [16] D. A. a. B. Singh, «Brain fingerprinting,» *Journal of Engineering and Technology Research*, vol. 4, n. 6, pp. 98-103, 2012.
- [17] D. R e D. K. K. Jayavardhanan, «Brain Fingerprinting,» *International Journal of Advanced Research in Computer Science and Technology*, vol. 3, n. 3, 2015.
- [18] F. L.A., «Brain MERMERs: Detection of FBI Agents and crime-relevant information with the Farwell MERA system.,» in *Proceedings of the International Security Systems Symposium*, ,Washington, D.C., 1993.
- [19] F. LA e R. DC, «Brain Fingerprinting in Laboratory Conditions.,» *Psychophysiology*, vol. 43, n. S38, 2006b.
- [20] S. S., « What you don't know can't hurt you,» *Law Enforcement Technology*, 2005.

[21] P. I. Series, *Brain Fingerprinting: Ask the Experts*, 2004.

[22] J. R. Evans, C. A. Meissner, S. E. Brandon, M. B. Russano e S. M. & Kleinman, «Criminal versus HUMINT interrogations: The importance of psychological science to improve interrogative practices,» *Journal of Psychiatry & Law*, n. 38, pp. 215-249, 2010.

[23] S. M. Kassin e G. H. & Gudjonsson, «The psychology of confessions: A review of the literature and issues,» *Psychological Science in the Public Interest*, n. 5, p. 33–67, 2004.

Main technology providers

NAME	HEADQUARTER	PRODUCTS - SERVICES	CLIENTS and COLLABORATORS	LINK	FIELDS OF APPLICATION
BrainwaveScience	Southborough, Massachusetts, (US)	iCognitive	Clients: Victoria Police (Melbourne, Australia), National Information in Ministry of Interior (Saudi Arabia), Central Bureau of Investigation (India)	https://brainwavescience.com/	National Security, Law Enforcement, Counterterrorism, Border Security, Human and Drug Trafficking, Immigration
Brain Fingerprinting Laboratories Inc.	Seattle, Washington, (US)			https://farwellbrainfingerprinting.com/	National Security, Law Enforcement, Counterterrorism, Border Security, Human and Drug Trafficking, Immigration
Nielsen Holdings Inc.	New York (US)		Clients: Coca-Cola Company, NBC Universal, Nestle S.A., The Procter & Gamble Company, Twenty-First Century Fox Inc., Unilever Group.	https://www.nielsen.com/it/	Neuro-marketing, Audience measurements
SPARK Neuro	New York, (US)	SPARK PLATFORM combines the power of brain signals (EEG) with advanced deep-learning techniques to decode brain activity signals. Our software allows experts and non-experts alike the ability to test patients with the push of a button, automatically running test protocols and generating reports.	Collaborators: Mayo Clinic (Minnesota,US), Department of Defence (US), U.S. Air Force, Alzheimer's Disease Research Center (ADRC), New York University, University of California, and University of Massachusetts.	https://www.sparkneuro.com/	Alzheimer's Disease diagnosis, Brain Injuries, Cognitive Disorders

REPORT (set2022) <https://www.futuremarketinsights.com/reports/brain-fingerprinting-technology-market>