NOTIONES

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

D5.5

Monitoring of EU Research and Horizon Scanning -v4

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

Project Details

Acronym: **NOTIONES**

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

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

Reference: 101021853

Type: Coordination and support action

Program: HORIZON 2020

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

Topic-ID: SU-GM01-2020

Start: 01.09.2021 – 31.08.2026

Duration: 60 months

Consortium:

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

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
30	BEYOND THE HORIZON	BTH	Belgium

Deliverable Details

Number: **D5.5**

Title: **Monitoring of EU Research and Horizon Scanning -v4**

Lead beneficiary: Z&P

Work package: WP5

Dissemination level: PU (Public)

Nature: Report (RE)

Due date: 31st October 2023

Submission date: 30th October 2023

Authors: **Giulia Venturi, Maria Ustenko,** Z&P
Livia Di Bernardini, Claudio Testani, APRE;

Contributors:

Reviewers: **Sirra Toivonen**, VTT; **Ciro Caterino**, Exp.AI

Version History:

Date	Version No.	Author	Notes
01/09/2023	0.1	Z&P	ToC
22/09/2023	0.11	Z&P	Section 3.4, Section 1
29/09/2023	0.2	APRE	Section 3
03/10/2023	0.3	Z&P	Section 2.2
17/10/2023	0.4	Z&P	Section 2.1
20/10/2023	0.5	Z&P	Section 4, Section 5
27/10/2023	0.55	VTT, EXP.AI	Internal review
30/10/2023	1.0	Z&P	Update after review - finalized
30/10/2023	1.1	TECNA	Final version to be submitted

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

Table of Content

List of Figures

List of Tables

Acronyms

ABE	Attribute Based Encryption
AI	Artificial Intelligence
BSA	Backtracking Search optimization Algorithm
BVLOS	Beyond Visual Line of Sight
CCIS	Crime and Criminal Information System
CCTNS	Crime and Criminal Tracking Network & Systems
CCTV	Closed-circuit television
CI	Critical Communication Infrastructures
CORDIS	Community Research and Development Information Service
CSA	Coordination and Support Action
D&A	Detect and Avoid
DL	Deep Learning
DLT	Distributed Ledger Technologies
EC	European Commission
EMIF	European Media and Information Fund
ENVI	Environment for Visualising Images
ERA	emergency response applications
ESC	Electronic Speed Controller
EU	European Union
FICN	Fake Indian Currency Notes
GDPR	General Data Protection Regulation
GNN	Graph Neural Networks
GNSS	Global Navigation Satellite System
IIoT	Internet of Things
JRC	Joint Research Centre
NCRB	National Crime Records Bureau
PDC	private data collection
PNT	based positioning, navigation and timing
RTO	Research and Technology Organisation
SBVM	Secure Block Verification Mechanism

SC	Smart Contracts
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
UxV	Unmanned Aerial/Land/Naval etc. … Vehicles
VAE	Variational Autoencoder
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 M25 and M26 since the beginning of the project (fourth 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*. Datasets were explored searching for publications that may be of relevance for the upcoming NOTIONES working groups: blockchain solutions, and drones/UxVs.

Section 2.2 reports on the research activities carried out in task T5.2 "*Research monitoring on EU projects"* through cascade refinement stages of research on CORDIS, to identify the most interesting projects in terms of relevance for the upcoming NOTIONES working groups: blockchain, tools for privacy-enhancing processing of data, and drones/UxVs.

This section also presents an update about research projects for one of the current NOTIONES *focus areas* "disinformation validation".

Section 4 contains a summary of the most relevant findings of both tasks T5.2 and T5.3 through the common layout for the summarisation of the information proposed in deliverable D5.1. The following research projects and technologies are presented and their possible exploitation in NOTIONES is proposed: joint use of SDN and Blockchain technology, spectral search and discovery tool, Autofly project, and SAFIR-Ready project.

Section 5 contains conclusive considerations and next steps.

1. Introduction

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

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 i**nnovation monitoring**, defined as the activity aimed at gaining understanding of important technological trends, along with their intelligence and security implications, by finding and interpreting the available information in order to provide a concrete benefit to the NOTIONES network of stakeholders.

This document represents the product of the fourth run of tasks T5.2 and T5.3 of WP5, which performed the research monitoring activities during M25 and M26, as depicted in Figure 1.

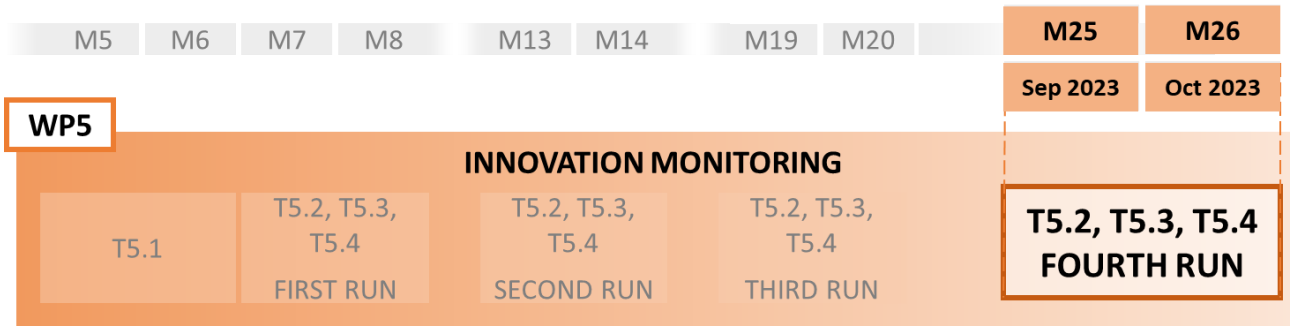

Figure 1 - Time diagram of the fourth run of innovation monitoring in WP5

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

- T5.2 Research monitoring on EU projects: this task will perform a deep survey of the emerging technologies that are the most promising in the field of intelligence and security by exploiting the great variety and volume of knowledge produced by EU research projects. To this purpose, the project will rationalize and categorize knowledge exploiting the CORDIS database as a primary source for information. In addition to this, the expertise of all NOTIONES partners will be exploited.
- T5.3 Research monitoring through Horizon Scanning: this task will perform a deep survey of the emerging technologies that are the most promising in the field of intelligence and security by exploiting the great variety and volume of knowledge openly available. To this purpose, the project will rationalize and categorize knowledge exploiting open databanks of publications and patents. The gathering of information will be performed by a targeted search based on the keywords, by means of technology horizon scanning. "Horizon scanning" is intended as

systematic research of relevant technological developments with the purpose of highlighting opportunity and threats that may influence the capability of organizations and bodies providing intelligence and security services to achieve their objectives ad goals. Such analysis should also consider the maturity level of technologies, so to identify whether it is at research phase, development, prototyping or production.

It is worth reminding that task T5.4 "*Monitoring of emerging terrorist threats*" reports the findings in a separate deliverable, namely D5.14 "*Monitoring of Emerging terrorist threats -v4*".

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 2.2 reports on the research activities carried out in task T5.2 "*Research monitoring on EU projects".*

Section 4 contains a summary of the most relevant findings of both tasks T5.2 and T5.3.

Section 5 contains conclusive considerations and next steps.

1.2 Focus areas

Before the start of the fourth run of tasks T5.2 and T5.3, as the WP5 leader Z&P began to plan the periodic monitoring activities, a discussion took place with the leaders of WP6, VTT and LAU, and the project coordinator TECNA. The subject of the discussion were the topics of the upcoming working groups, in order to direct the research of WP5 towards them.

Z&P identified some topics based on the needs collected in WP2, some requests that emerged with the passed WGs, as well as the outcomes of the finalized WPs, listed below:

- Big data analytics;
- Terrorism;
- Training;
- Cybersecurity/ cyber ranges;
- 3D printing;
- Drones;
- Cloud security;
- IoT security;
- Cyber intelligence tools;
- Digital forensic;
- Blockchain;
- Data fusion & integration platforms;
- Natural Language Processing;
- Social media analytics;
- Network analysis tools;

- GEOINT, Satellite imagery and remote sensing;
- Biometric identification.

The coordinator, after internal discussions and from the initial list of needs and requirements identified by practitioners, identified two additional focus areas that could add value to NOTIONES and deserved to be discussing further. These were:

- Technological solutions to secure data sharing and dissemination (internally and externally);
- Discussing technological solutions and improvements to the processing phase of the intelligence cycle.

It was originally proposed to share the list with the practitioners of the NOTIONES Consortium and make them choose the topics they wanted to work with. LAU pointed out that the initial planning of task T6.3 (new NOTIONES working groups) was scheduled for the beginning of September and that the first meetings would be focused on how to decide on the topics and how to organize the task in general. The decision about the topics of the new WGs would require much more time and involvement of the whole Consortium.

In the end, as the research of WP5 had to be done in September as the deliverables had to be submitted in October, the WP5 leader decided to focus the WP5 horizon scanning and research monitoring on the following topics:

- **Blockchain:**
  A blockchains is a distributed ledger with growing lists of records that are securely linked together via cryptographic hashes. Blockchain solutions were mentioned often in NOTIONES, e.g. in the presentation about the LOCARD and LAZARUS projects during the second NOTIONES workshop. The members of NOTIONES WG3 expressed particular interest in this topic.
- **Tools for privacy-enhancing processing of data:**
  This is an evergreen topic that is of interest for practitioners from the very first moment in NOTIONES, actually not just for privacy but also for secure data sharing and dissemination, with the considerations made by task T3.5 on big data and by task T3.6 on artificial intelligence.
- **Drones/UxVs:**
  The use of drones and unmanned vehicles raised interest in practitioners since the very beginning of NOTIONES with the work carried out in task T3.1 about technologies for IMINT and SIGINT, and with the work carried out by task T3.7 about mass surveillance. It was later also described during the first NOTIONES conference with practical use cases and applications to Intelligence and Security.

The coordinator agreed on the three topics selected for the horizon scanning and research monitoring, considered the limited time to perform the research and the fact that the proposed topics appeared to be of interest to practitioners. It was also agreed to update the research on the focus area of “AI for disinformation detection”, in support of the NOTIONES WG4.

2. Research monitoring through Horizon Scanning

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

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

For the fourth 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 (Community Research and Development Information Service) [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 Masters Degree 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 third run of WP5 are presented.

The focus areas tackled in this run of the horizon scanning task are the possible topics of the upcoming third round of NOTIONES Working Groups (see section 1.2):

- blockchain solutions;
- drones/unmanned vehicles.

The focus area "Tools for privacy-enhancing processing of data" could not be tackled in this run of task T5.3 as the results from the scientific publications and patents database are thousands, with the vast majority related to the management of health personal data, and the analysts could not extract substantial information for NOTIONES, even using clustering methods.

Also, the research about patents for blockchain solutions gave results about new architectures which do not appear as relevant for NOTIONES: Intelligence and security practitioners are perceived to be

more interested in the application of the blockchain solution in general, rather than on different architectures of the solution itself which is a purely technical consideration at this stage.

The initial research about patents for drones gave thousands of results both in patents and scholarly works, that not necessarily were relevant to the objectives of NOTIONES. In order, to make the analysis of the most recent results as well as relevant to the practitioners of NOTIONES, some filters were applied including the time range and the key words. This led to a certain number of only papers included result, while the patents were not present anymore.

2.1 Blockchain solutions

The first horizon scanning performed in the fourth run of task T5.2 took as a starting point the possible upcoming NOTIONES focus area about *blockchain solutions*.

The search on the online scholar database *TheLens* with keyword "*blockchain*" in search field title with no date range limit led to 58418 results with 2447 cited patents and 5534 citing patents.

It was decided to limit the range of search to allow for a manageable amount of data and for the most recent and relevant results. The search on the online scholar database *TheLens* with keyword "*blockchain*" and "*crime*" in all search fields, with date range limitation to 2022 and 2023, led to 259 results with no citing nor cited patents.

Among the results, several publications are about the use of distributed blockchains in relation to **digital evidence preservation** and **crime report management**.

Mehta et al. from the SRM Institute of Science & Technology in Chennai, India, propose a "*Blockchain driven Evidence Management System*" [3] to prevent offenses' records and chain of digital evidences to be hacked. The paper describes a blockchain solution able to handle the problem by encrypting and storing data as a hash along with the timestamp and hash of the next block. The data can be changed only with proof of work and a vote of consensus in which a majority of the blockchain must agree to the change. The hash is stored in smart contracts using Ethereum [4]. The study demonstrates a trade-off between the number of transactions contained in a single block on the blockchain ledger and the security level of various hashing algorithms for the offence data.

Shilpa and Shanthakumara from the Siddaganga Institute of Technology, in Tumakuru, India, report about "*An Implementation of Blockchain Technology in Combination with IPFS for Crime Evidence Management System*" [5] in order to realize tamper-proof chains of evidences protected from any kind of alterations. In order to build a strong system with immutability, integrity, and legitimacy features the authors state that the blockchain technology is the most suitable, since the digital evidence can be transferred in a transparent way between the parties involved without any central authority. This study also implements Ethereum [4].

Verma et al. from the Uttaranchal University in Dehradun, India, in their paper "*Blockchain and Cloud Computing used in Preservation of Crime Scene Evidences*" [6] identify that these technological innovations provide enhancement in data security as well as storage of data. Shetty et al. from the Datta Meghe College of Engineering in Arioli, India, also explore the opportunities of "*Crime Evidence Over Blockchain*" [7] .

Amin et al. from the Faridpur Engineering College in Bangladesh, in collaboration with the University of Regina in Saskatchewan, Canada, proposes a "*Blockchain Interoperable Crime Report Management*

System By Utilizing Hyperledger Cacti & Private Data Collection (PDC)" [8]. Such system serves especially for sharing information and sensitive data related to a certain case involving international law enforcement cooperation. The proposed blockchain-based interoperable crime management system provides secure and decentralized communication between different blockchain-based platforms, ensuring anonymity, transparency, and immutability. It can be used for crime reporting, evidence management, forensic testing, collaboration between investigation agencies, and resource sharing where users can report in two modes: anonymous mode, which is only for passing any information to the authorities, or generate mode, which will create a First Information Report and subsequent procedures. The system uses Hyperledger Cacti [9] to implement interoperability and allows investigation and collaboration with others, like courts, forensics, and special investigation agencies, even with foreign systems. This proposed system is effective and efficient, enhancing the performance of blockchain networks.

Another solution is explored by Anand Karambe from the Shri Rawatpura Sarkar University in Raipur, India, in his work "*Blockchain-Based Approach for Tracking Global Criminals*" [10]. The author stresses the importance of Blockchain solutions due to their tamper-proof security, as each transaction is stored in an immutable distributed ledger on each blockchain node. The paper explains that Investigative agencies can have difficulties in locating and researching the past of criminals who committed crimes in another Country. This problem may be solved if investigative agencies had a common global criminal database and applications to extract information. This would reduce the time for the investigation and would eliminate the possibility of falsification and tamper with criminal records.

A similar solution relating to "*Criminal Records and Reporting System*" is proposed by Sonkamble et al. from the JSPM Narhe Technical Campus in Maharashtra, India [11]. The study aims to contribute to the security protocol of criminal record data through Blockchain, focusing on the security protocols that prevent unlawful changes in the data.

Bhalerao et al. from the D.Y. Patil University in Mumbai, India, in their paper "*Block Crime: Criminal Incidence Detection Using Facial Recognition Based on Concepts of Blockchain"* [12] propose to deploy police servers on a website whose transactions are monitored on a blockchain server. The backend of this server utilizes Ganache (a tool for creating a local Ethereum blockchain [13]) to store such blocks of ethers. The authors propose to use this system for the application of video surveillance using CCTV cameras installed in public and private places, followed by biometric recognition to detect the suspects of a crime scene, done through use of the OpenCV library [14] and using the biometric features based on their Identity card (Aadhaar card). Hence, the pictures captured on the camera would be processed and sent to authorities along with individual details.

It is evident that this field of research is particularly present in India, where the National Crime Records Bureau (NCRB) [15] provides the Indian Police with Information Technology and Criminal Intelligence also in the form of national databases and platforms such as the Crime and Criminal Information System (CCIS) and the Crime and Criminal Tracking Network & Systems (CCTNS). The NCRB collects, collates, and disseminates information on Crime, Criminals, Persons and Property for matching purposes though the use of the following the software systems:

- VahanSamanvay - An online Motor Vehicle Coordination System for coordination of stolen and recovered motor vehicles across the country. Police, RTOs, and Insurance sector are main stakeholders. The general public is also benefited with this system.
- Talash Information System - This system is used to maintain and coordinate information on Missing, Traced, Unidentified persons and unidentified dead bodies.

- Fake Indian Currency Notes System (FICN) - It is an online system for compilation of fake Indian currency data. Police, Bbanks, investigating agencies, other intelligence agencies and Ministries are stakeholders of this system.
- Fire Arms Coordination System - This system is used for coordination of missing/stolen and recovered firearms.
- Colour Portrait Building System - This system is used to create portraits of suspects based on the description given by victims and eyewitnesses.

In addition to this, India possesses a centralized database called Aadhaar which represents the world's largest biometric database with data on over 1.1 billion people. The already-mentioned Aadhaar card is a 12-digit identification document that can be obtained by any resident of India and that requires the submission of biometric data in the form of fingerprints and iris scan. Facial-recognition technology is routinely implemented by the Indian law enforcement agencies also thanks to the extensive presence of CCTV cameras.

With a slightly different approach, Rathore et al. from various universities in India describe "*An evolutionary algorithmic framework cloud based evidence collection architecture*" [16], where they propose an automated forensic platform leveraging Infrastructure as a Cloud Service based on the Blockchain concept.

All the data is stored and encrypted in a cloud server where homomorphic encryption (a form of encryption that allows computations to be performed on encrypted data without first having to decrypt it) is implemented. Secure Block Verification Mechanism (SBVM) is proposed to safeguard the server from unauthorized access, using the Backtracking Search optimization Algorithm (BSA, a population-based evolutionary algorithm for numerical optimization problems) to strengthen the cloud environment and optimally generate secret keys.

The cloud computing adopts the Software-Defined Networking (SDN) technology. A block in the SDN controller is created for every data and a hash-based tree is constructed in each block by Secure Hash Algorithm (SHA). Graph Neural Networks (GNN) enhanced Smart Contracts (SC) are then implemented to enable users to track their data. Finally, the construction of an evidence graph using the blockchain data enables evidence analysis. The authors carried out experiments and claim to have obtained good results according to a comprehensive comparative study.

With regard to Smart Contracts enhanced by GNNs, it is not clear how Rathore et al. used GNNs. It may be speculated that they used GNNs to detect vulnerabilities in the SC as proposed by Zhuang et al. [17].

With regard to the joint use of SDN and Blockchain technology, this was already extensively studied by other authors, for example Rahman et al. in their paper "*On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives*" [18]. The authors notice that the integration of Blockchain with SDN provides improved manageability, transparency, and security of applications thanks to its tracked, audited, and (if needed) publicly accessible data, as well as transaction transparency, personal data protection, legitimacy, compliance, and trust. However, the authors warn that although there a lot of opportunities and advantages, on the joint use of these technologies, there are also technical challenges when they are applied in scenarios having particular constraints in terms of scalability and computational efficiency. Thus, there is room for further research effort for the improvement of security and performance of Blockchain–SDN also in view of upcoming use cases and possible threats.

A possible threat is represented by Ransomware. Abuomar et Yale Gross from the Lewis University in Romeoville, Illinois, USA, propose "*Using Blockchain, RAID, & BitTorrent Technologies to Secure Digital*

Evidence from Ransomware" [19] to mitigate ransom attacks from destroying months or years of generated digital evidence and to break up the digital evidence that has been generated to prevent the blockchain from getting too large and slowing down the system as more blocks are added to the chain.

Akello et al. from the University of Texas at San Antonio, USA, in their work "*Blockchain Use Case in Ballistics and Crime Gun Tracing and Intelligence: Toward Overcoming Gun Violence*" [20] propose a management system for gun-related data from the point of manufacture/sale, as well as at points of transfers between secondary sellers for the improvement of criminal investigation processes.

2.2 Drones/unmanned vehicles

The second horizon scanning performed in the fourth run of task T5.2 took as a starting point the possible upcoming NOTIONES focus area about *drones/unmanned vehicles*.

The initial search on *TheLens*, an online scholarly database, using the keyword "unmanned vehicles" in the title field without specifying a date range, yielded a total of 18013 scholar work results, including 32 cited patents and 34 citing patents.

Subsequently, it was determined that the search results needed to be refined to a more manageable dataset, focusing on the most recent and relevant information. Therefore, a refined search was conducted on *TheLens*, using the keywords "unmanned vehicles" AND "crime" in all search fields, with a date range limited between Dec 2021 and Sept 2023. This refined search produced a more focused set of 38 results, with no citing or cited patents found within this specific timeframe.

Unmanned vehicle may be substituted by its synonyms drones or UAVs (Unmanned Aerial Vehicles) or RPAS (Remotely Piloted Aerial Systems).

Defence applications for UAVs

The article [21] suggests that the use of a swarm of unmanned vehicles, primarily micro-UAVs can significantly impact the defense sector, particularly in protecting high-value assets like military bases. Through testing and demonstrating autonomous swarms composed of various types of vehicles, the study highlights the potential benefits of such systems. Key developments focus on reducing uncertainties in situational awareness information by employing computationally efficient algorithms for mobile sensor tasking, sensor fusion, information fusion, and behavior monitoring. The research demonstrates that these technologies can be integrated into commercially available unmanned vehicles, offering real-time situational awareness, aiding decision-making, and reducing mission costs and human exposure to threats in defense applications.

This text [22] discusses the potential impact of Unmanned Aircraft Systems (UAS) on the service industry, with a projected value of 71 billion USD by the end of the decade. It emphasizes the importance of autonomous Beyond Visual Line of Sight (BVLOS) operations enabled by robust Detect and Avoid (D&A) capabilities. Currently, BVLOS operations in the UK and EU are limited, hindering the development of D&A technology. The paper highlights legal liabilities for remote pilots, even when complying with regulations, and addresses the need for certification processes tailored to software-intensive UAS products. It also advocates for standards and infrastructure to demonstrate the competency of autonomous UAS, with implications for civil, criminal, and privacy laws. The authors engage with regulators to influence UAS-related laws and policies and conduct research on sensor capabilities for detection.

Use for crime detection and forensic

Unmanned aerial vehicles have proven valuable in various forensic scenarios, such as detecting clandestine graves, aiding evidence detection in outdoor crime scene investigations. They offer increased accuracy, speed, and versatility, with the possibility of further enhancement through computer vision techniques. Drones can overcome environmental obstacles like air gaps and dense vegetation to locate sub-surface anomalies or burial sites. They offer non-intrusive, cost-effective, and time-efficient benefits, especially in capturing high-resolution aerial imagery. These technologies can improve the efficiency of investigations, facilitate access to challenging areas, especially in conflict zones, and enhance the collection of evidence and samples from crime scenes. Recently many studies were registered with the scope to underscore the importance of integrating modern technologies, particularly UAVs, into forensic investigations and law enforcement practices. The research findings suggest that drones can play a significant role in improving the efficiency and effectiveness of crime scene investigations when compared to traditional human methods. Namely, Tychyna et al in their study [23] aim to provide practical recommendations for incorporating UAVs into pre-trial investigations, in order to significantly enhance forensic activities and the work of law enforcement agencies.

The article [24] explores the versatile applications of drones in forensic science. Mohd Sabri et al suggest utilizing near infrared cameras for victim identification during the crime scene investigations. The scientist proved empirically that NIR reflectance helps identify disturbed soil from non-disturbed soil and differentiate healthy vegetation from stressed vegetation. This is particularly useful when searching for clandestine graves, as changes in soil and vegetation patterns may indicate their presence. The use of drone-mounted sensors enhances evidence detection beyond human vision, and multi-sensor platforms can be developed with specialized expertise.

Krekeler et al made their attempt to aid security community in their daily duties. The scientist developed [25] a freely available "*Spectral search and discovery tool*" to aid in forensic investigations, search, rescue, and emergency response operations, particularly in outdoor settings. The primary goal of this tool is to provide software for the interpretation of hyperspectral remote sensing images. These spectra can be interpreted to identify objects in the images. The tool also has the potential to document large disaster, crime, or conflict scenes, allowing for the tracking of changes over time and conducting forensic analyses. Additionally, a library with extensive metadata supporting material identification has been created for the ENVI (Environment for Visualising Images) remote sensing platform, which is used in conjunction with this tool. The library contains data related to various materials and can support the identification of substances, making it a valuable resource for law enforcement, or security practitioners.

This study investigates the role of drones in real-time evidence detection at outdoor crime scenes [26]. The authors state that integrating computer vision enhances drones' capabilities further in near-perfect detection rates, scan large areas swiftly, and work effectively across diverse terrains. This study explores the role of UAVs in real-time evidence detection in outdoor crime scene investigations. It seeks to determine the effectiveness of drones compared to traditional human methods in detecting objects of interest in a simulated crime scene. Innovative findings highlight the remarkable potential of drones in crime scene investigations. DJI SPAR drones, when configured with appropriate flight settings, can achieve exceptionally high detection rates, approaching 100%, rendering them highly effective at pinpointing objects of interest during investigations. They also offer the advantage of expediting searches, covering large areas more swiftly than human teams, resulting in substantial reductions in required man-hours. Moreover, drones exhibit consistent detection capabilities across

diverse terrains, enhancing their reliability for outdoor crime scene investigations. The integration of MATLAB computer vision toolbox and other techniques further augments their detection capabilities, potentially improving accuracy and real-time evidence detection. However, it's crucial to ensure stable communication data links for successful drone deployment, as signal degradation or loss can impact coverage and investigation outcomes.

Use for surveillance, tracking, patrolling, detection

There are many articles that discuss the widespread use of UAVs in various industries, including their potential to revolutionize businesses and create new opportunities. UAVs are employed for tasks such as surveillance, supply chain management, and acting as mobile hotspots [27].

Hardik Sachdeva et al identify that UAVs are vulnerable to cyberattacks and misuse by malicious entities, posing risks to data, property, and even human lives. To address these challenges, the authors propose securing UAV communication using blockchain technology. The approach involves creating smart contracts to establish a secure and reliable UAV ad-hoc network. This network is designed to withstand various network attacks and defend against malicious intrusions, offering potential benefits to industries and businesses relying on drone technology. Key elements include ensuring data privacy through encryption, maintaining data integrity via blockchain's immutability, establishing trust between network nodes through token exchanges and Ethereum guarantees, and bolstering security against a range of attacks, such as blackhole, gray hole, DoS, confidentiality, and integrity attacks. The article also provides valuable experimental results and discussions, demonstrating the effectiveness of this blockchain-based system in enabling remote control of UAV mobility and coordinates.

Ingale et al. have innovatively developed an unmanned aerial vehicle boasting a range of features [28]. These drones, equipped with object detection capabilities, open up a realm of applications in crime control, leveraging attributes like feature extraction and thermal signatures. What sets them apart is their autonomy, enabling operation in otherwise inaccessible areas, enhancing security. Drones are celebrated for their efficiency, reliability, cost-effectiveness, and inherent security, making them invaluable for surveillance and monitoring. The components of this drone system encompass motors, ESC, Pixhawk, power distribution, battery, receiver, and camera, the latter being instrumental in capturing live information that is seamlessly broadcast to the pilot on the ground. Control can be exercised through remote control units or monitors, granting operators flexibility and versatility. These drones exhibit extended flight times, long-range control capabilities, and lifting capacity, with a potential to handle weights ranging from 500 to 700 kg, a testament to their utility in rescue and logistics operations. The results achieved by this designed quadcopter system are remarkable: it can sustain 50 minutes of continuous flight, operate effectively at a remote-control range of 2 km, engage in live video transmission, object detection, and face recognition. The system's incorporation of object shape comparison further enhances its detection capabilities, rendering it highly applicable to real-life scenarios. In addition to its functionality, a 3D printed case serves to protect the system's components from crashes, while an emergency return feature ensures the drone can safely return to its take-off location. While certain sensor range limitations exist, they are mitigated by the system's overall stability and satisfactory performance. The designed quadcopter system also reveals potential for application in real-life scenarios, extending its utility to assisting stranded individuals and performing various surveillance tasks.

The proliferation of unregistered UAVs has resulted in numerous incidents, including disturbances at international airports and increasing UAV-related crimes. To address this issue, radio technology has emerged as an efficient early warning method for detecting unregistered UAVs. Traditional methods of UAV detection based on remote control signals have faced technical challenges, such as susceptibility to environmental noise, complexity, and low accuracy [29]. While, Zhang et al introduce

a novel approach to UAV remote control signal detection using cyclic spectrum features. The authors begin by constructing a dataset of UAV remote control signals in the frequency domain (UAV-CYCset). Based on this dataset, they propose a network architecture based on an improved AlexNet. Through simulation experiments, the improved model achieves an average detection accuracy of 85% across signal-to-noise ratios ranging from -10 dB to 10 dB.

The article presents a new technology [30] in the form of a steerable sensor platform designed for small-scale unmanned aerial vehicles operating in urban environments. The proposed platform allows for the effective integration of sensors, enabling obstacle avoidance and target tracking capabilities. Unlike conventional rigid sensor placements, this movable platform offers greater flexibility, reduces weight constraints, simplifies sensor integration, and minimizes costs. Additionally, the design of the platform ensures that it does not induce aerodynamic instability during UAV operation. The technology provides a solution to enhance the autonomy and sensing capabilities of small-scale UAVs for urban law enforcement and surveillance missions.

Liu et al present an innovative approach for unsupervised anomalous event detection in videos, particularly those captured by UAVs. This method [31] leverages contextual information derived from visual characteristics to address the semantic gap that often exists between visual data and the interpretation of atypical incidents. The four key components of this method include:

1. Contextual Graph: The method constructs a spatio-temporal contextual graph to represent various aspects of visual information. This graph encodes information about object manifestations, their relationships within the spatio-temporal domain, and scene categorization. It serves as a powerful representation of context in the visual data.

2. Transformer with Message Passing: Context information is encoded using a Transformer with message passing. This allows for the effective updating of the graph's nodes and edges, enabling the incorporation of context into the abnormal event detection process.

3. Graph-Based Deep Variational Autoencoder (VAE): A graph-oriented deep VAE approach is designed for the unsupervised categorization of scenes. This VAE helps in clustering different scenes based on their context and enables the accurate detection of anomalies that are context-dependent and may have ambiguous sources.

4. Improved Discrimination: By incorporating contextual information and scene clustering, the method enhances the discrimination between normal and abnormal events, making it particularly effective for detecting anomalies in UAV-captured videos.

The combination of these components allows for a novel approach to identify anomalous occurrences in video data, especially in scenarios where traditional supervised methods may not be practical or possible. This approach is especially valuable for UAV-based surveillance and other applications where context plays a critical role in detecting abnormal events.

Ryusei et al present a novel framework called "*watch-from-sky*" that uses multiple UAVs to perform predictive police surveillance. These UAVs play four key roles: sensing, data forwarding, computing, and patrolling. The framework relies on machine learning technology for controlling and dispatching UAVs and predicting crimes [32]. It leverages the mobility of UAVs, cloud infrastructure, and data-driven crime prediction to improve patrolling and deter crime. The paper also discusses the use of reinforcement learning for dispatching UAVs and distributed machine learning inference over lossy UAV networks. The article addresses the reduction in police and security forces in various parts of the world and how cloud-enabled infrastructures with UAVs and machine learning can enhance patrolling capabilities. It highlights that UAVs equipped with image sensors can effectively deter a wide range of

crimes, both inside and outside buildings. The watch-from-sky framework adapts UAVs for optimal utilization in crime deterrence, including sensing, data processing, and patrolling tasks.

To conclude the discussion, it may be noted that the utilization of unmanned aerial vehicles by law enforcement agencies for various purposes is a complex subject. It emphasizes both the advantages and challenges associated with employing drones for policing while underscoring the information-centric nature of law enforcement operations. UAVs offer substantial benefits in enhancing law enforcement activities, serving as effective aerial surveillance tools for crime prevention, detection, investigation, and safeguarding national security interests. They find application in a range of scenarios, from search and rescue missions to crime scene investigations and handling hostage situations. However, the deployment of drones in certain situations, such as crowd monitoring and during protests, can be a source of contention, as it potentially encroaches on various human rights, including the right to privacy, data protection, free speech, the right to protest, and freedom of movement. The ethical and legal dimensions of police drone usage come to the fore, emphasizing the need to address these concerns [33]. The issue at hand is not the technology itself but how the data gathered is processed and acted upon. Striking a balance between the benefits of UAVs for public safety and the potential drawbacks, particularly concerning government surveillance without adequate safeguards, is a crucial task. Furthermore, this discussion explores the variances in legal positions and regulations across different countries, presenting diverse approaches and legal frameworks in the United States, the United Kingdom, France, and South Africa. The conversation delves into specific ethical and legal aspects, including the necessity for purpose-specific legislation, warrant requirements for drone deployments, the use of drones in protests and crowd monitoring, the admissibility of drone-gathered evidence, the possibility of armed or weaponized drones, and the constitutional implications of drone policing on privacy and data protection. This multifaceted exploration ultimately underscores the importance of implementing safeguards, ensuring transparency, and upholding accountability in police drone usage to maintain public trust and protect human rights. By incorporating clear guidelines and safeguards, law enforcement agencies can harness the benefits of drone technology while mitigating the associated risks and public distrust.

Legal aspects

Technology has a remarkable tendency to advance rapidly, pushing the boundaries of what's possible and reshaping various aspects of our lives. However, this rapid progress often outpaces the development of legal regulations designed to govern its use. Thus, it's important to emphasize the lack of standardized practices for drones in forensic applications, the inadequacy of drone ethics and legal regulations, as well as the limited understanding and awareness of drone utilization. The lack of standardized practices for drones in forensic applications can be attributed to several factors, i.e rapid technological advancements. Drone technology has been evolving rapidly, with new models and capabilities emerging frequently. This fast-paced development makes it challenging to establish standardized practices that can keep up with. Secondly, unmanned vehicles are used in a wide range of forensic applications, from crime scene analysis to search and rescue missions. Each of these applications has unique requirements, making it difficult to create a one-size-fits-all standard. Also, due to the fact that regulatory environment for drones is still evolving in many regions. Different countries and jurisdictions may have varying rules and guidelines for drone usage, adding complexity to the establishment of standardized practices. Another reason to the absence of the standardized practices may be limited research and awareness, as without comprehensive studies and a clear understanding of best practices, which makes it challenging to develop standards. Finally, drones in LEAs or security practitioners' applications can raise ethical and privacy concerns, especially when they

are used for surveillance or data collection. Addressing these concerns in standardized practices requires careful consideration.

Nonetheless, many efforts are ongoing to address these challenges and establish guidelines and standards for drone usage in forensic contexts, but it remains an evolving field. In example, Siong discusses the use of drones by law enforcement agencies in Malaysia and the legal issues surrounding their utilization, highlighting the need for comprehensive regulations [34]. To address these concerns, the authors recommend a proactive approach to the regulation and use of drones, with a focus on legality, ethics, and ensuring that technology benefits society without compromising individual rights and security. In the article the following three pillars approach is suggested:

1. Strengthening Legal Oversight: to cover the necessity for robust legal frameworks and regulations governing the use of drones by law enforcement agencies to ensure that drone operations are conducted within legal boundaries, respecting individuals' privacy rights and national security concerns.

2. Comprehensive Regulation: The authors call for comprehensive regulations that not only govern law enforcement's use of drones but also cover security practitioners and civilian drone operations.

3. Balancing Security and Privacy: it is suggested that regulations should strike a balance between enhancing national security and safeguarding individuals' privacy. This balance is crucial to prevent potential abuses of drone technology while allowing law enforcement agencies to effectively carry out their duties.

The authors Tuliov et al as well emphasize that modern law-making and law enforcement agencies cannot effectively perform their functions without the adoption of legislative regulators [35]. According to the researchers, to enhance law enforcement's ability to combat high-tech crimes and protect citizens' rights and national security, the widespread adoption of modern technologies is crucial. The implementation of these innovative technologies, including UAVs, is guided by international treaties, EU resolutions, and national legislation, which collectively shape the legal framework for their use in law enforcement agencies, with the specific mix varying from country to country. However, the only regulatory document in the EU, a 2015 resolution from the European Parliament, focuses on security, privacy, and mandatory pilot registration data on chips for UAVs. Thus, the scientists propose a methodological scheme that combines theoretical and empirical research methods with documentary systems and analysis.

Osiecki et al in their research focus on the legal implications and challenges associated with the use of UAVs in civil and military contexts, and provide the proposals for updating international law include addressing liability for the use of drones against humanitarian law and cyberattacks targeting UAVs [36]. The authors discuss the need to adapt and update international legal frameworks to address the unique challenges posed by UAVs, particularly in the context of terrorism and counter-terrorism and modern warfare. By exploring the primary aspects of UAV usage from a legal perspective, the authors also note that UAVs used in civil air transport are susceptible to terrorist attacks. Terrorist organizations may target unmanned aircraft, posing a threat to passengers and global aviation security. The article highlights the vulnerability of UAVs to hacking and remote hijacking, as demonstrated in experiments by government agencies. Osiecki et al conclude that, UAVs, whether used for civilian or military purposes, are subject to existing international aviation laws.

The research of Yefimenko from 2022, highlights that existing legislation governing the use of UAVs by law enforcement is formal and insufficient in addressing new challenges posed by evolving crime methods and technological advancements [37]. The study analyzes international experiences of law

enforcement agencies in technologically advanced countries, such as the USA, Great Britain, Germany, France, China, and Israel, in employing UAVs. It also considers the potential integration of Ukrainian-designed UAVs into the National Police's operations. The research emphasizes the practical benefits of using UAVs, including enhanced efficiency in law enforcement tasks, cost-effectiveness, and improved safety, while also recognizing the need for precise regulation to mitigate potential risks and ensure compliance with the law. UAVs have technical capabilities that enable effective crime prevention and monitoring of roadways, pipelines, and railway transport, thanks to their ability to capture real-time data in various spectral ranges enhances surveillance capabilities, especially in low-visibility conditions. While UAVs offer substantial benefits, their use must be carefully regulated to prevent misuse and potential harm to individuals, society, and the state. The author invites the legislators to consider amending existing laws and regulations to provide clear guidelines for the use of UAVs by law enforcement agencies.

3. Research monitoring on EU projects

A search on the European Community CORDIS Platform 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, second and third runs 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 dataset retrieval was obtained by searching on the CORDIS database the research projects mentioning keywords related to the possible topics of the upcoming third round of NOTIONES Working Groups (see section 1.2):

- blockchain solutions;
- tools for privacy-enhancing processing of data;
- drones/unmanned vehicles.

The research was performed by Ms. Livia di Bernardini and by Mr. Claudio Testani of Consortium partner APRE.

Mr. Testani (Orcid ID: 0000-0002-5312-6016, Hi=13) 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.

Ms. Di Bernardini holds a Master of Arts in International Relations (Università degli Studi Roma Tre) with focus on the Common Security and Defence Policy (CSDP) of the EU and a second level Master's degree in Cybersecurity, Public policy, regulation and management (Luiss Guido Carli University). She is currently employed at APRE where she carries out several projects in the framework of the Horizon Europe cluster 4 "Digital, Industry and Space".

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

3.1 Blockchain

With regards to the search of EU-funded project dealing with "blockchain" technology, the search on the CORDIS database revealed 55 results by filtering the field to "security". The manual refinement of the results led to a total of 9 projects considered relevant for NOTIONES, shown in the table below:

Table 1 Selected projects based on the keyword "blockchain"

Acronym	Title	Start - end year	Mapped at
OntoChain	Trusted, traceable and transparent ontological knowledge on blockchain	2020-2023	4th round
INSPECTr	Intelligence Network and Secure Platform for Evidence Correlation and Transfer	2019-2023	2nd and 4th round
CRITICAL-CHAINS	IOT- & Blockchain-Enabled Security Framework for New Generation Critical Cyber-Physical Systems in Finance Sector	2019-2022	4th round
LOCARD	Lawful evidence collecting and continuity platform development	2019-2022	4th round
C4IIoT	Cyber security 4.0: protecting the Industrial Internet of Things	2019-2022	4th round
COBAFRA	Combatting Banking Fraud with SiS-id: A unique solution for preventing corporate payments fraud using AI and blockchain	2019	4th round
RESISTO	RESIlience enhancement and risk control platform for communication infraSTructure Operators	2018 - 2021	4th round
ALOHA	Software framework for runtime-Adaptive and secure deep Learning on Heterogeneous Architectures	2018 - 2021	4th round
TITANIUM	Tools for the Investigation of Transactions in Underground Markets	2017-2020	1st - 4th round

The mentioned EU-funded projects underscore a comprehensive approach to fortifying security and privacy across varied domains. They are pioneering in integrating advanced technologies such as blockchain and machine learning to fortify the integrity and reliability of transactions, combat cybercrimes, and secure sensitive data.

NGI OntoChain and CRITICAL-CHAINS are specifically focusing on establishing decentralized reputation models and secure cyber-physical systems to ensure trustworthy transactions and combat illicit activities. LOCARD is addressing the challenges associated with maintaining the integrity and privacy of digital evidence in criminal investigations, providing solutions that are crucial for law enforcement and intelligence agencies.

Projects like C4IIoT are developing robust cybersecurity frameworks for the Industrial Internet of Things (IIoT), integrating advanced protection mechanisms and blockchain technologies to safeguard industrial technologies. COBAFRA is innovatively addressing bank transfer fraud by deploying platforms that integrate AI and blockchain to authenticate transactions and secure banking identities online.

These projects are not only enhancing the security infrastructure in sectors like healthcare, finance, and industrial automation but are also trying to set new standards in data protection and privacy, ensuring user-centric approaches and compliance with stringent data protection regulations. The innovations and solutions derived from these projects have the potential to create enhanced capabilities and tools that are highly relevant for security and intelligence operations, ensuring a more secure and trustworthy digital ecosystem.

Below is reported a synthesis of main information about the projects.

3.1.1 OntoChain

Project	OntoChain
Full Title	Trusted, traceable and transparent ontological knowledge on blockchain
GRANT AGREEMENT ID	957338
Source of information	https://cordis.europa.eu/project/id/957338
EU contribution	6.011.100,00 €
Coordinator	European Dynamics Luxembourg Sa
Website	ONTOCHAIN project Home | ONTOCHAIN (ngi.eu)
Call for proposal	H2020-ICT-2018-20
Start Date	1 September 2020
End Date	31 August 2023

The EU-funded NGI OntoChain project is focused on enabling trustworthy transactions of services and content through innovative business models. These models aim to generate value, a portion of which is returned to the blockchain community as compensation for contributing computational resources. The project is developing decentralized reputation models to uncover the quality and types of services and the credibility of data sources, maintaining a balance between privacy and trust. It seeks to create reliable and traceable content, allowing authorized parties to process data in accordance with the owners' policies. OntoChain is set to demonstrate its capabilities in sectors like eHealth, eGovernment, eEducation, and eCommerce, aiming to establish an economically sustainable ecosystem.

The objective of OntoChain is to capitalize on the growing number of Internet-based marketplaces and the emergence of cryptocurrencies and smart contracts. It aims to facilitate the deployment of new services with low-entry market barriers due to minimal infrastructure costs and decentralized, secure transaction management. The project is designed to meet the trust requirements of companies and organizations by enabling them to understand their user base, verify identities, manage digital assets, and control trust issuance within their ecosystems.

The project seems to be relevant in the security and intelligence field as the development of decentralized reputation models can aid in assessing the credibility of data sources and services, essential for intelligence gathering and analysis. Its application in sectors like eGovernment and its ability to facilitate the deployment of new, secure services can contribute to enhancing the overall security infrastructure and protocols within intelligence agencies and other security-related organizations. The traceability and reliability of content provided by OntoChain are considered also pivotal for ensuring the integrity and authenticity of information in security operations.

3.1.2 INSPECTr

Project	INSPECTr
Full Title	Intelligence Network and Secure Platform for Evidence Correlation and Transfer (INSPECTr)
GRANT AGREEMENT ID	833276
Source of information	https://cordis.europa.eu/project/id/833276

EU contribution	€ 6.997.910,00
Coordinator	University College Dublin, National University Of Ireland - Dublin
Website	https://inspectr-project.eu/
Call for proposal	H2020-SU-SEC-2018
Start Date	1 September 2019
End Date	28 February 2023

This project has been already outlined in the 2nd round of this task and reported in D5.3. It appears to be a highly pertinent initiative as it seeks to create a unified intelligence platform designed to enhance digital and forensic capabilities while diminishing the complexity and expense associated with cross-border collaboration.

3.1.3 CRITICAL-CHAINS

Project	CRITICAL-CHAINS
Full Title	IOT- & Blockchain-Enabled Security Framework for New Generation Critical Cyber-Physical Systems In Finance Sector
GRANT AGREEMENT ID	833326
Source of information	https://cordis.europa.eu/project/id/833326
EU contribution	4.182.154,25 € out of 4.985.547,50 €
Coordinator	THE UNIVERSITY OF READING – UK
Website	Critical Chains - (reading.ac.uk)
Call for proposal	H2020-SU-DS-2018
Start Date	1 July 2019
End Date	30 September 2022

The EU-funded CRITICAL-CHAINS project developed solutions to enhance security and privacy in cyber-physical systems used in sectors like banking and insurance. The project introduces a triangular accountability model and a multi-layered, cloud-based "X-as-a Service" framework to combat illicit transactions, fraud, and money trafficking in FinTech e-operations. It incorporates advanced features like data integrity checking through blockchain, threat intelligence, multilateral biometric-based authorization, and hardware security module (HSM) enabled security. The model will be validated across critical sectors, assessing its reliability, usability, and compliance with various standards. The consortium leading this initiative combines diverse expertise and includes stakeholders from different sectors to ensure a comprehensive approach to cyber-physical system challenges.

The project's innovative triangular accountability model and advanced features like blockchain for data integrity and multilateral biometric-based authorization address critical security concerns such as illicit transactions, fraud, and money trafficking. These solutions are crucial for intelligence agencies to monitor, detect, and combat financial crimes and cyber threats effectively.

Report on lessons learnt and final recommendations: Report on lessons learnt and final recommendations

3.1.4 LOCARD

Project	LOCARD
Full Title	Lawful evidence collecting and continuity platform development

GRANT AGREEMENT ID	832735
Source of information	https://cordis.europa.eu/project/id/832735
EU contribution	833.385,00 €
Coordinator	Athina-Erevnitiko Kentro Kainotomias Stis Technologies Tis Pliroforias, Ton Epikoinonion Kai Tis Gnosis
Website	-
Call for proposal	H2020-SU-SEC-2018
Start Date	1 May 2019
End Date	31 July 2022

The EU-funded LOCARD project is addressing the challenges associated with the use of digital evidence in criminal investigations. Given the prevalence of digital tools in various crimes, including fraud, terrorism, and intellectual property theft, LOCARD aims to develop a holistic platform to ensure the proper chain of custody and integrity of digital evidence. The platform will utilize a 'Trusted Execution Environment' and blockchain technology to guarantee the privacy, source, and integrity of the evidence, allowing it to be admissible in court. LOCARD's platform will allow each node to set permission policies and share access to digital evidence selectively, ensuring flexibility and adaptability to the specific needs of diverse actors in the forensic workflow. It will feature modules for citizen reports of violations, detection and correlation of online deviant behavior, and a toolkit for investigators to assist in collecting both online and offline evidence. The use of immutable storage and an identity management system will further enhance the security and privacy of the digital evidence collected, allowing interoperability without the need for a trusted third party. Thus, it has the potential to be a reliable tool for law enforcement and intelligence agencies.

Main results:

A Framework for Supply Chain Traceability Based on Blockchain Tokens
Author(s): Thomas K. Dasaklis, Fran Casino, Costas Patsakis, Christos Douligeris
Published in: Business Process Management Workshops - BPM 2019 International Workshops, Vienna, Austria, September 1–6, 2019, Revised Selected Papers, Issue 362, 2019, Page(s) 704-716, ISBN 978-3-030-37452-5
Publisher: Springer International Publishing
DOI: 10.1007/978-3-030-37453-2_56

SoK: Blockchain Solutions for Forensics
Author(s): Dasaklis, T.K., Casino, F., Patsakis, C.
Published in: Security Informatics and Law Enforcement, 2021, ISBN 978-3-030-69460-9
Publisher: Springer
DOI: 10.1007/978-3-030-69460-9_2

Testing and Validation Outcomes

A public report that will evaluate the implementation of the LOCARD pilot deployments including satisfaction of demonstrators with the implementation and its possible improvements provide a global picture of security issues produce a global estimate of the financial costs and benefits and investigate success factors leading to the maximal effectiveness of LOCARD.

3.1.5 C4IIoT

Project	C4IIoT
Full Title	Cyber security 4.0: protecting the Industrial Internet Of Things
GRANT AGREEMENT ID	833828
Source of information	https://cordis.europa.eu/project/id/833828
EU contribution	4.993.533,75 € out of 6.288.708,75 €
Coordinator	Idryma Technologias Kai Erevnas - Greece
Website	https://www.c4iiot.eu/
Call for proposal	H2020-SU-ICT-2018
Start Date	1 June 2019
End Date	31 May 2022

The EU-funded C4IIoT project is focused on enhancing cybersecurity within the Industrial Internet of Things. It aims to develop a unified IIoT cybersecurity framework to anticipate, detect, and mitigate malicious and anomalous behaviors, thereby minimizing the attack surfaces in IIoT systems. This framework integrates advanced protection mechanisms, machine and deep learning, privacy-aware analytics, encrypted network flow analysis, secure-by-design IIoT device fabrication, and blockchain technologies. These integrations aim to provide a comprehensive security solution, preserving privacy, enabling reliability, and assuring trustworthiness within IIoT applications. The C4IIoT framework will undergo testing and validation in real-world environments, focusing on inbound logistics and a smart factory, to demonstrate its effectiveness in addressing the increased risk of cyberattacks, disruptions, data loss, and industrial espionage inherent in IIoT systems.

The development of a unified IIoT cybersecurity framework addresses critical security concerns arising from the integration of various industrial technologies.

3.1.6 COBAFRA

Project	COBAFRA
Full Title	Combatting Banking Fraud with SiS-id: A unique solution for preventing corporate payments fraud using AI and blockchain
GRANT AGREEMENT ID	835813
Source of information	https://cordis.europa.eu/project/id/835813
EU contribution	50.000,00 € out of 71.429,00 €
Coordinator	SIS - France
Website	https://sis-id.com/en/
Call for proposal	H2020-SMEInst-2018-2020-1
Start Date	1 January 2019
End Date	30 June 2019

The EU-funded COBAFRA project address the escalating issue of bank transfer fraud, particularly supplier fraud, through the commercialization of a collaborative platform, My Sis ID. This platform, designed by CFOs and treasurers, focuses on the identity aspect of the payment process, ensuring payments are directed to the correct company and safeguarding companies' banking identities online. It integrates with existing systems of customers and suppliers and employs artificial intelligence and blockchain to enhance traditional data-pooling and enrollment models. The platform aims at ensuring secure and authenticated transactions, which is essential for intelligence agencies monitoring financial activities.

My Sis ID offers secure solution, developed in collaboration with 13 pioneer customers, to meet the pressing need for fraud prevention in corporate banking, with no similar comprehensive solutions currently existing in the market. It operates on a viral business model, allowing customers and suppliers to invite their respective suppliers and customers to the platform, promoting widespread adoption. The platform, launched in November 2017, has intentions for cross-border deployment due to the borderless nature of fraud, indicating considerable market potential in Europe and beyond.

3.1.7 RESISTO

Project	**RESISTO**
Full Title	RESIlience enhancement and risk control platform for communication infraSTructure Operators
GRANT AGREEMENT ID	786409
Source of information	https://cordis.europa.eu/project/id/786409
EU contribution	7.999.970,00 € out of 10.531.803,71 €
Coordinator	LEONARDO
Website	http://www.resistoproject.eu/
Call for proposal	CIP-2016-2017-2
Start Date	1 May 2018
End Date	31 October 2021

The RESISTO project is an innovative platform designed to enhance the resilience and situational awareness of Critical Communication Infrastructures (CIs). Recognizing the pivotal role of communications in societal and economic well-being, and the vulnerabilities they face from criminal activities, extreme weather events, and the complexities introduced by evolving technologies like 5G, the project aims to address these challenges. RESISTO offers an Integrated Risk and Resilience analysis, covering all resilience cycle phases such as preparation, prevention, detection, and absorption. It employs cutting-edge technologies like Blockchain, Machine Learning, IoT security, and holistic audio-video analytics to protect against combined cyber-physical threats. The platform's Decision Support System, built on a Software Defined Security model, enables Communication Operators to implement mitigation actions and countermeasures, reducing the impact of adverse events. This ensures efficient recovery to original and operational states, minimizing performance losses, social consequences, and cascading effects.

The RESISTO platform is relevant in the field of security and intelligence as it addresses the critical need for enhanced resilience and protection of CIs which are primary targets for criminals and are vulnerable to both cyber-physical threats and natural disasters.

3.1.8 ALOHA

Project	ALOHA
Full Title	software framework for runtime-Adaptive and secure deep Learning On Heterogeneous Architectures
GRANT AGREEMENT ID	780788
Source of information	https://cordis.europa.eu/project/id/780788
EU contribution	5.976.415,00 €

Coordinator	STMICROELECTRONICS SRL – Italy
Website	https://www.aloha-h2020.eu/
Call for proposal	H2020-ICT-2017-1
Start Date	1 January 2018
End Date	30 June 2021

The ALOHA project aims to facilitate the implementation of Deep Learning (DL) algorithms on low-energy, heterogeneous computing platforms, addressing the challenges posed by the shift to the edge computing paradigm. DL algorithms are highly effective in various tasks like recognition and classification but deploying them on edge devices requires balancing performance requirements with power/energy consumption constraints. This pose challenges due to the need for advanced skills and significant effort in programming for heterogeneous architectures.

ALOHA intends to develop a software development tool flow to automate algorithm design and analysis, optimize the porting of inference tasks to embedded architectures, and implement middleware to control the target platform for optimal power and energy savings. The tool will address several features including architecture-awareness, adaptivity, security, productivity, and extensibility, considering the limitations and features of the embedded architecture from the design phase. The project has been assessed in various application domains including surveillance, smart industry automation, and medical applications, to validate its effectiveness in enabling the deployment of DL algorithms in diverse scenarios with varying constraints and requirements.

The ability to implement DL algorithms on low-energy, heterogeneous computing platforms can significantly enhance the capabilities of edge devices in surveillance and intelligence gathering. The optimized deployment of DL algorithms can aid in real-time recognition, identification, and classification tasks, which are crucial in security operations and threat detection.

3.1.9 TITANIUM

Project	TITANIUM
Full Title	Tools for the Investigation of Transactions in Underground Markets
GRANT AGREEMENT ID	740558
Source of information	https://cordis.europa.eu/project/id/740558
EU contribution	4.991.600 €
Coordinator	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH, Austria
Website	Startseite - AIT Austrian Institute Of Technology
Call for proposal	H2020-SEC-2016-2017-1
Start Date	1 May 2017
End Date	30 April 2020

The EU-funded TITANIUM project is developed advanced, legally compliant tools to aid law enforcement in investigating cybercrimes involving cryptocurrencies. The project has produced a suite of open-source, privacy-preserving forensic tools designed for analyzing data associated with darknet markets and virtual currency transactions. These tools, available to any law enforcement team, are undergoing rigorous testing and will be provided as open-source solutions or products supported by European SMEs, with training sessions to ensure proper use. The initiative ensures adherence to EU data privacy regulations, including the GDPR, and aims to equip European law enforcement with the

necessary tools to more effectively and efficiently investigate and combat cybercrimes involving virtual currencies. The project has been already mapped in the in NOTIONES D5.2, D5.3 and D5.4.

Main results – peer reviewed articles:

The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates†
Author(s): Markus Riek, Rainer Böhme
Published in: Journal of Cybersecurity, Issue tyy004, 2018, Page(s) 1, ISSN 2057-2085
Publisher: Oxford University Press
DOI: 10.1093/cybsec/tyy004

The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments
Author(s): Stearns Broadhead
Published in: Computer Law & Security Review, Issue in press, 2018, Page(s) Volume 34, Issue 6, December 2018, Pages 1180-1196, ISSN 0267-3649
Publisher: Pergamon Press Ltd.
DOI: 10.1016/j.clsr.2018.08.005

Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements
Author(s): Paulina Jo Pesch, Christian Sillaber
Published in: Computer Law Review International, Issue 18/6, 2017, Page(s) 166 ff., ISSN 2194-4164
Publisher: De Gruyter
DOI: 10.9785/cri-2017-0602

Virtual Currencies and Fundamental Rights
Author(s): Christian Rueckert
Published in: SSRN Electronic Journal, Issue Journal of Cybersecurity 2019, Vol. 5, No. 1, 2019, ISSN 1556-5068
Publisher: Oxford University Press
DOI: 10.2139/ssrn.2820634

Safeguarding the evidential value of forensic cryptocurrency investigations
Author(s): Michael Fröwis, Thilo Gottschalk, Bernhard Haslhofer, Christian Rückert, Paulina Pesch
Published in: Forensic Science International: Digital Investigation, 2020, Page(s) 200902, ISSN 2666-2817
Publisher: Elsevier ScienceDirect
DOI: 10.1016/j.fsidi.2019.200902

Bitcoin and Cybersecurity: Temporal Dissection of Blockchain Data to Unveil Changes in Entity Behavioral Patterns
Author(s): Francesco Zola, Jan Lukas Bruse, Maria Eguimendia, Mikel Galar, Raul Orduna Urrutia
Published in: Applied Sciences, Issue 9/23, 2019, Page(s) 5003, ISSN 2076-3417
Publisher: Mdpi
DOI: 10.3390/app9235003

3.1.10 Other projects

During the research, it was noted that some EU-funded projects use blockchain technologies to ensure more privacy-conscious data processing primarily focused on the healthcare sector. Some of these initiatives are included in the table below as the technologies they use can also be potentially interesting in the context of NOTIONES.

Table 2 Further projects to be monitored

Project Identification	Scope and Application	Potential Impact
PANACEA: Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people **Grant Agreement ID:** 826293 **Link:** https://cordis.europa.eu/project/id/826293	enhance cybersecurity in the healthcare sector by developing and implementing comprehensive, people-centric solutions	enhanced cybersecurity protocols, more effective dynamic risk assessment, and innovations in secure information sharing
MH-MD: My Health - My Data **Grand Agreement ID:** 732907 **Link:** http://www.myhealthmydata.eu/	address challenges of data subjects' privacy and data security in the biomedical sector by implementing a distributed, blockchain-based, peer-to-peer architecture	Innovative blockchain-based data protection, ensuring tighter control over sensitive information and enhancing trust and transparency in data exchanges
CUREX: seCUre and pRivate hEalth data eXchange **Grant Agreement ID:** 826404 **Link:** https://cordis.europa.eu/project/id/826404	enhance healthcare data security by developing a decentralized, private blockchain-based architecture that enables healthcare providers to assess and address cybersecurity and privacy risks optimally	blockchain-based solutions to assess and mitigate cybersecurity and privacy risks, ensuring optimal data protection and integrity, which are crucial in handling sensitive information in intelligence operations

3.2 Tools for privacy-enhancing processing of data

When the research on the CORDIS platform focused on privacy-enhancing tools, 148 projects were initially identified. After an evaluation based on relevance to the NOTIONES project, ten projects were selected and listed in the table below.

Table 3 Selected projects based on the keywords "privacy" and "security"

Acronym	Title	Start - end year	Mapped at
DataVaults	Persistent Personal Data Vaults Empowering a Secure and Privacy Preserving Data Storage, Analysis, Sharing and Monetisation Platform	2020 - 2023	4th round
TRAPEZE	TRAPEZE - TRAnsparency, Privacy and security for European citiZEns	2020 - 2023	4th round

ARCAone	Next generation security platform to safeguard critical applications and sensitive digital assets	2019 - 2020	4th round
LPS	For a full data privacy on the go	2019 - 2020	4th round
PRIViLEDGE	Privacy-Enhancing Cryptography in Distributed Ledgers	2018 - 2021	4th round
PAPAYA	PlAtform for PrivAcY preserving data Analytics	2018 - 2021	4th round
PDP4E	Methods and tools for GDPR compliance through Privacy and Data Protection Engineering	2018 - 2021	4th round
DEFeND	Data Governance for Supporting GDPR	2018 - 2021	4th round
cyberwatching.eu	The European watch on cybersecurity privacy	2017 - 2021	4th round
ENCASE	EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors	2016 - 2019	4th round

These projects illustrate an effort within the European Union to advance the field of security and privacy through innovation, collaboration, and technology integration. The emphasis on user-centric, holistic, and compliant solutions across diverse domains underscores the multifaceted nature of security and privacy challenges and the need for comprehensive and adaptable strategies to address them.
In particular, the following findings are highlighted:

- Many projects, like ENCASE and PDP4E, develop user-centric solutions aimed at empowering individuals and organizations with tools and methodologies to protect their data and privacy, emphasizing the importance of user involvement and awareness in cybersecurity.
- The integration of advanced technologies such as blockchain, artificial intelligence, and deep learning is a common approach in these projects to address security and privacy challenges, showcasing the pivotal role of technology in developing innovative solutions for data protection.
- Projects like TRAPEZE are adopting holistic and integrated approaches to address security and privacy concerns, emphasizing the need for comprehensive solutions that consider various aspects and levels of the digital ecosystem.
- Several projects, like PAPAYA and DEFeND, are focusing on ensuring compliance with regulations like the GDPR, highlighting the importance of legal frameworks in shaping and guiding the development of privacy and security solutions.
- The projects span diverse domains including healthcare, finance, and industrial sectors, indicating the widespread relevance and applicability of security and privacy solutions across different fields and industries.
- The collaboration between different countries and sectors is evident in these projects, showcasing the importance of cross-border and inter-sectorial cooperation in addressing global and multifaceted challenges in security and privacy.

Below is reported a synthesis of main information about the projects.

3.2.1 DataVaults

Project	DataVaults
Full Title	Persistent Personal Data Vaults Empowering a Secure and Privacy Preserving Data Storage, Analysis, Sharing and Monetisation Platform
GRANT AGREEMENT ID	871755
Source of information	https://cordis.europa.eu/project/id/871755
EU contribution	5 999 995,00 € out of 7.664.755,00 €
Coordinator	Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev
Website	https://www.datavaults.eu/
Call for proposal	H2020-ICT-2019-2
Start Date	1 January 2020
End Date	30 April 2023

The EU-funded DataVaults project is addressing the growing needs of Europe's burgeoning data economy for trusted, secure, and ethically driven personal data platforms and privacy-aware analytics methods. The project is developing a framework and platform centered around personal data from diverse sources, defining secure, trusted, and privacy-preserving mechanisms. This enables individuals to have ownership and control over their data, allowing them to share it willingly through flexible data sharing and fair compensation schemes with other entities.

The objective of DataVaults is to overcome the challenges hampering the growth of the data economy, such as the lack of secure and ethical personal data platforms and methods that can securely share personal and proprietary data while fairly defining value capture, production, release, and monetization for the benefit of all stakeholders.
DataVaults focuses on providing extra functionalities and methods on its personal data platform to retain data ownership, safeguard security and privacy, notify individuals of their risk exposure, and secure value flow based on smart contracts. The approach aims to rejuvenate the personal data value chain, envisioning it as a multi-sided and multi-tier ecosystem governed and regulated by smart contracts, which safeguard personal data ownership, privacy, usage, and attribute value to the data producers.
The EU-funded DataVaults project is developing a secure and ethical framework and platform focusing on personal data from various sources, aiming to empower individuals with ownership and control over their data. The project addresses the challenges in the data economy, including privacy, security, and ethical concerns, by establishing secure and privacy-preserving mechanisms and allowing individuals to share their data willingly through flexible and fair compensation schemes. DataVaults aims to facilitate enhanced collaboration between data owners and seekers, focusing on safeguarding privacy, security, and data ownership, and utilizing smart contracts to govern and regulate the personal data value chain.

Main results available:

- Updated DataVaults Security Methods and Market Design
  This deliverable presents the technical background of private smart contracts and their application in DataVaults, in particular for the Access Policy Engine, Attribute Based Encryption (ABE) and Searchable Symmetric Encryption (SSE).

- DataVaults MVP and Usage Scenarios

The DataVaults integrated methodology revealing how components and concepts interrelate and displaying high level usage scenarios of the concept formulating the platforms MVP to provide input to the use cases the architecture and specification tasks in WP3 WP4 WP5.

- Personal Data Market Design, Contracts and Rules
  An analysis of the stateoftheart approaches towards the definition of value flows of data economies as well as data monetization compensation mechanisms of DataVaults SotA approaches of personal data management using for smart contracts and DLT.

3.2.2 TRAPEZE

Project	**TRAPEZE**
Full Title	TRAPEZE - 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 out of 6.017.950,00 €
Coordinator	TENFORCE
Website	TRAPEZE (trapeze-project.eu)
Call for proposal	H2020-SU-DS-2019
Start Date	1 September 2020
End Date	31 August 2023

The TRAPEZE project is focused on enhancing the cyber resilience of the European data space, acknowledging the pivotal role of data in societal and economic development. It aims to develop innovative technologies that allow citizens to have active control over their security and privacy, thereby contributing to the resilience of the data space. The initiative is designed to instil a sense of trust in the European data economy by redefining concepts of control, transparency, and compliance through innovations that prioritize citizens.

TRAPEZE plans to utilize advanced technologies like Blockchain and Linked Data to ensure data integrity and legal compliance, offering protection against malicious entities and providing a clear overview of transborder data flows. The project emphasizes direct involvement of European citizens in the development of technologies enhancing security and privacy, ensuring usability and co-production. It is driven by real-world use cases and combines extensive EU-funded research in security and privacy to create practical and marketable solutions, aiming to lead global initiatives in delivering privacy-aware innovations.
The emphasis on citizen involvement, transparency, and compliance in developing privacy-aware innovations addresses security needs, making TRAPEZE a valuable initiative in the security and intelligence sector.

3.2.3 PRIViLEDGE

Project	PRIViLEDGE
Full Title	Privacy-Enhancing Cryptography in Distributed Ledgers
GRANT AGREEMENT ID:	780477
Source of information	https://cordis.europa.eu/project/id/780477
EU contribution	4.518.827,50 €

Coordinator	GUARDTIME OU
Website:	priviledge-project.eu
Call for proposal	H2020-DS-LEIT-2017
Start Date	1 January 2018
End Date	30 June 2021

The prevalent DLTs, despite being rooted in cryptography, do not inherently support privacy, posing a challenge for applications dealing with sensitive data like trade secrets and personal information. There is a need for advanced cryptographic techniques and protocols to safeguard data and fulfil the potential of DLTs in applications requiring privacy. The PRIViLEDGE project is addressing this gap by developing cryptographic protocols that support privacy, anonymity, and decentralized consensus for DLTs. It brings together leading European entities specializing in cryptographic research, fintech, and blockchain to advance the capabilities of cryptographic protocols for enhanced privacy and security.

The outcomes of the PRIViLEDGE project are showcased through four DLT-based solutions, including verifiable online voting, contract validation and execution for insurance, a ledger for university diploma records, and an update mechanism for stake-based ledgers. These use cases are chosen for their diversity and represent the primary application areas of DLT, ensuring that the advancements made in PRIViLEDGE have broad implications and impacts beyond the immediate scope of the project.

3.2.4 PAPAYA

Project	PAPAYA
Full Title	PlAtform for PrivAcY preserving data Analytics
GRANT AGREEMENT ID	786767
Source of information	https://cordis.europa.eu/project/id/786767
EU contribution	2.949.417,50 € out of 3.763.130,00 €
Coordinator	EURECOM GIE - France
Website	https://www.papaya-project.eu/
Call for proposal	H2020-DS-SC7-2017
Start Date	1 May 2018
End Date	31 July 2021

The EU-funded PAPAYA project is addressing the growing concerns around data privacy and the need for compliance with the European GDPR in the context of data analytics. The project aims to develop a platform of modules designed to protect user privacy on an end-to-end basis while still enabling the effective processing of data, even by untrusted third parties. The platform will allow data owners to extract valuable, meaningful, and useful information from protected (i.e., encrypted) data in a cost-effective and reliable manner, addressing the challenges posed by sensitive data analytics.

PAPAYA is focused on creating privacy-preserving data analytics primitives and will integrate these with auditing and visualization modules to increase trust in third-party data processors and ensure GDPR compliance. The developed solutions will be validated through real-world applications, including healthcare analytics and web & mobile data analytics, ensuring their applicability and effectiveness in addressing privacy risks and enhancing data protection in various domains.

3.2.5 PDP4E

Project	PDP4E

Full Title	Methods and tools for GDPR compliance through Privacy and Data Protection Engineering
GRANT AGREEMENT ID	787034
Source of information	https://cordis.europa.eu/project/id/787034
EU contribution	2.941.113,13 € out of 3.362.457,22 €
Coordinator	TRIALOG
Website	https://www.pdp4e-project.eu/
Call for proposal	H2020-DS-SC7-2017
Start Date	1 May 2018
End Date	30 April 2021

The PDP4E project aimed at providing engineers with methods and tools to integrate data protection principles into their projects, ensuring compliance with the GDPR. It focuses on integrating privacy and data protection functionalities into existing mainstream, primarily open-source, software tools within the Eclipse ecosystem, using a model-driven engineering approach. The methodologies integrated are derived from both the privacy engineering community and the software and system engineering industry.

The project seeks to embed privacy and data protection into various engineering disciplines like Risk Management, Requirements Engineering, Model-Driven Design, and Assurance. The effectiveness of PDP4E has been assessed through demonstration pilots in industries where privacy is crucial, specifically in connected vehicle applications and big data on smart grids.

Main results available:

Risk management methods for data protection and privacy v2
This document will describe the risk management method, including all methodological elements besides the tool. The document will be revised in M23 to adapt the method to the feedback received from stakeholders.

Specification and design of model-driven design tool for privacy and data protection v3
This document will provide the detailed design of the tool for data protection and privacy model-driven design tool. A first version will be delivered in M14, which will be revised in M18 and M33 introducing the insights from the validation activities.

Specification and design of requirements engineering tool for data protection and privacy v3
This document will provide the detailed design of the tool for data protection and privacy requirements engineering. A first version will be delivered in M14, which will be revised in M18 and M33 introducing the insights from the validation activities.

3.2.6 DEFeND

Project	DEFeND
Full Title	Data Governance for Supporting GDPR
GRANT AGREEMENT ID	787068
Source of information	https://cordis.europa.eu/project/id/787068
EU contribution	2.737.300,00 € out of 3.325.910,37 €
Coordinator	ATOS SPAIN SA, Spain
Website	https://www.defendproject.eu/
Call for proposal	H2020-DS-SC7-2017

Start Date	1 July 2018
End Date	31 March 2021

The DEFeND project aimed to develop a platform that assists organizations in various sectors to assess and achieve GDPR compliance and enhance their maturity in different aspects of GDPR. This platform is developed to enable organizations to build and analyze models with a Privacy-by-Design approach at both the Planning and Operational Levels, covering Data Scope, Data Process, and Data Breach management areas. The project will leverage existing software, tools, and methodologies to implement platform software components.

The DEFeND platform undergone testing in living labs pilots in four EU countries, focusing on healthcare, banks, energy, and local public administration, and has be evaluated in operational environments across different scenarios focusing on GDPR compliance for end-users and implications for external stakeholders.

Main result available:
Functional testing report
Presentation of the technical testing plan and its results, describing also Quality-of-Service testing for the platform and delivery of a list of recommended changes for improving the platform. Connected Task(s): Task 4.3

3.2.7 cyberwatching.eu

Project	cyberwatching.eu
Full Title	The European watch on cybersecurity privacy
GRANT AGREEMENT ID	740129
Source of information	https://cordis.europa.eu/project/id/740129
EU contribution	1.999.895,63 €
Coordinator	Trust-It Services Limited - UK
Website	Cyberwatching
Call for proposal	H2020-DS-SC7-2016
Start Date	1 May 2017
End Date	31 July 2021

The cyberwatching.eu project aims to establish an EU Observatory to monitor Research & Innovation (R&I) initiatives focused on cybersecurity and privacy across the EU and Associated Countries. The project clustered such initiatives using a cluster tool and identify themes, resulting in an online catalogue of cybersecurity and privacy services. This catalogue showcased market uptake and contributed to advancing EU's sustainable competitiveness by creating a supply and demand marketplace for EU cybersecurity products and services. The inclusion of an end-users' club ensures the perspectives of SMEs and other stakeholders are considered, aiming to create a comprehensive cybersecurity and privacy ecosystem.

The main outputs of the project include a continuously updated observatory and R&I online catalogue, a cluster tool, multiple meetings, workshops, webinars, cluster reports, white papers, and roadmaps. The project aims for sustainability through the creation of a cybersecurity and privacy marketplace, offering prime and guided access to the cyberwatching.eu catalogue of services and ensuring feedback regarding the effectiveness and usability of research results.

3.2.8 ARCAone

Project	ARCAone
Full Title	Next generation security platform to safeguard critical applications and sensitive digital assets
GRANT AGREEMENT ID	888406
Source of information	https://cordis.europa.eu/project/id/888406
EU contribution	50.000,00 € out of 71.429, 00 €
Coordinator	CYSEC SA - Switzerland
Website	https://www.cysec.com/
Call for proposal	H2020-SMEInst-2018-2020-1
Start Date	1 December 2019
End Date	31 March 2020

The EU-funded ARCAone project address the critical need for enhanced cybersecurity in the digital age, focusing on developing a combined hardware and software solution to ensure secure digital execution and storage. This solution is designed to protect various data resources, including cryptocurrencies, cryptographic keys, and other sensitive data, and is aligned with existing security models, sophisticated security protocols, and regulatory demands.

ARCAone, developed in response to high-profile cybercrimes and data breaches, offers a secure and compliant environment for various digital assets, providing broad functionality and future-proof solutions. Since its foundation in May 2018, the project has raised €1.4m and earned €246,000 in beta sales, with the team having experience in developing secure software like OpenBSD & OpenSSH.
The commercialization strategy of ARCAone involves developing vertical applications built on the platform, starting with the financial segment and IoT, before expanding to cloud services and other segments. The project aims to involve third-party developers to build applications, allowing the focus to remain on the ARCAone SDK and application marketplace, and achieving scale through third-party applications.

3.2.9 LPS

Project	LPS
Full Title	For a full data privacy on the go.
GRANT AGREEMENT ID	886716
Source of information	https://cordis.europa.eu/project/id/886716
EU contribution	50.000,00 € out of 71.429,00 €
Coordinator	DEVPRIV - France
Website	https://www.allpriv.com/
Call for proposal	H2020-SMEInst-2018-2020-1
Start Date	1 October 2019
End Date	29 February 2020

The EU-funded LPS project, led by AllPriv, developed innovative nomadic cybersecurity solutions aimed at protecting data privacy outside the office environment. This initiative is crucial due to the increasing prevalence of remote work and the associated risks, such as connecting to unsecured Wi-Fi and potential device loss, which pose significant security threats to enterprises. The project seeks to

miniaturize an entire security stack into a portable hardware format, embedding advanced technologies like blockchain and artificial intelligence to offer comprehensive protection.

AllPriv's approach has garnered attention from large enterprises and has undergone paid testing with Europe's third-largest bank. The company is working to overcome significant technological challenges to develop groundbreaking technology and has filed six patents, demonstrating its commitment to achieving its objectives.

3.2.10ENCASE

Project	ENCASE
Full Title	EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors
GRANT AGREEMENT ID	691025
Source of information	https://cordis.europa.eu/project/id/691025
EU contribution	2.160.000,00 €
Coordinator	TECHNOLOGIKO PANEPISTIMIO KYPROU - Cyprus
Website	https://encase.socialcomputing.eu/
Call for proposal	H2020-MSCA-RISE-2015
Start Date	1 January 2016
End Date	31 December 2019

The ENCASE project' objective was to protect minors from malicious actors in online social networks by leveraging advances in usable security and privacy. It will implement a user-centric architecture, consisting of three browser add-ons, to form a protective net against cyberbullying and sexually abusive acts. The first add-on detects aggressive or distressed behavior; the second one analyzes social web data to detect fraudulent activity and alerts the user; while the third warns users or their parents when sensitive content is about to be shared with an inappropriate audience, offering controls to protect content through watermarking, cryptography, or steganography.

The project combines academic and industrial expertise, focusing on user experience assessment, large-scale data processing, machine learning, and content confidentiality techniques, with real-world online social network data and production-grade software development. The add-ons and back-end software undergone user studies and piloting activities before public release, fostering knowledge exchange through an interdisciplinary secondment program for researchers.

Main results available:

- Report on user and societal aspects, and on usability of security and privacy OSN systems
  Report on user and societal aspects, and on usability of security and privacy OSN systems
- System requirements and software architecture (a)
  System requirements and software architecture intermediate report
- System requirements and software architecture (b)
  System requirements and software architecture final report

- Development of automated techniques to detect early indications of malicious behavior of social network users
  Development of automated techniques to detect early indications of malicious behavior of social network users

- Security- and privacy-driven user interface design guidelines
  Security- and privacy-driven user interface design guidelines

3.3 Drones/UxVs

The field of Drones, Unmanned Vehicles and Related Technologies generated many funded projects within EU Horizon Europe programme: the search on the CORDIS database revealed 49 projects initially, which were reduced to 32 by filtering the starting date (from January 2020) and the end date (2022 at least). Some of these projects were found to cover very specific goals, such as agriculture monitoring or forest alerts mapping, which although being very promising have small or no impact/interest for the NOTIONES project. Other projects, even if focused on general applications, may provide interesting inputs to NOTIONES.

Twelve projects were finally selected based on their relevance for security and intelligence practitioners. These projects are reported in the table below.

Table 4 Selected projects based on the keywords "Drones/UxVs"

Acronym	Title	Start - end year	Mapped at
I-SEAMORE	Integrated Surveillance Ecosystem for European Authorities Responsible for Maritime Operations Leveraged by Reliable and Enhanced Aerial Support	2023 - 2025	4th round
AUTOFLY	GPS-Free, Beyond the Visual Line of Sight Navigation for Logistics Drones in Urban Environments	2022 - 2023	4th round
ODYSSEUS	Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation	2023 - 2025	4th round
URANUS	Real-Time Urban – Mobility Management Via Intelligent Uav-Based Sensing	2023 - 2028	4th round
EGeNiouSS	EGNSS-based Visual Localisation to enable AAA-PNT in small devices & applications	2022 - 2026	4th round
SAFIR-Ready	Obtain Flight Mission Readiness, Enabling Rapid Intervention for Healthcare and Critical Infrastructure, Leveraging All Value Chain Actors and U-Space Services	2023 - 2026	4th round
COVER	Cooperative And Intelligent Unmanned Aerial Vehicles for Emergency Response Applications	2023 - 2026	4th round
OVERWATCH	Integrated holographic management map for safety and crisis events	2022 - 2025	4th round
THRUST	Substituting Helicopters with Climate-Friendly Fixed-Wing Drones for Infrastructure Inspection	2022 - 2023	4th round
EMERITUS	Environmental Crimes' Intelligence and Investigation Protocol Based On Multiple Data Sources	2022 - 2025	4th round

HAIKU	Human AI teaming Knowledge and Understanding for aviation safety	2022 - 2025	4th round
MAGDA	Meteorological Assimilation from Galileo and Drones for Agriculture	2022 - 2025	4th round

Below is reported a synthesis of main information about the projects.

3.3.1 I-SEAMORE

Project	I-SEAMORE
Full Title	Integrated Surveillance Ecosystem For European Authorities Responsible For Maritime Operations Leveraged By Reliable And Enhanced Aerial Support
GRANT AGREEMENT ID	101073911
Source of information	https://cordis.europa.eu/project/id/101073911
EU contribution	6.481.677,32 € out of 7.995.929,38 €
Coordinator	ATOS IT SOLUTIONS AND SERVICES IBERIA SL
Website	-
Call for proposal	HORIZON-CL3-2021-BM-01
Start Date	01/01/2023
End Date	30/06/2025

The EU-funded I-SEAMORE project is focused on developing an advanced, holistic platform designed to enhance maritime surveillance operations and situational awareness for European authorities. The platform, intended to be operated from Maritime Operation Centres (MOCs), will host and manage several innovative assets, services, and systems, offering capabilities like wide maritime border and coastal area monitoring, threat analysis, support to search and rescue operations, and detection of illegal activities. The platform will integrate multiple types of long-endurance unmanned assets, exploit various data sources including payload data and open data sources like Copernicus Services, and utilize AI and Big Data Analysis for optimal decision-making and mission execution. I-SEAMORE platform focus on 4 main pillars: 1) employment and indirect tasking of multiple types of long-endurance Unmanned Assets (aerial and water surface), 2) exploitation of heterogeneous data sources e.g. payload data and open data sources including Copernicus Services, 3) provision of a common operational picture empowered by a novel and comprehensive suite of data fusion services based on AI and Big Data Analysis, for optimal decision making and successful mission execution of the desired missions, and 4) interoperability within the Ecosystem and its interface with key existing external systems.

The project aims to facilitate multi-country, multi-authority collaboration and will develop standard operating procedures, novel concepts of operation, and new methodologies for the co-creation and validation of maritime security solutions.

3.3.2 AUTOFLY

Project	AUTOFLY
Full Title	GPS-Free, Beyond the Visual Line Of Sight Navigation For Logistics Drones In Urban Environments
GRANT AGREEMENT ID	190185259
Source of information	https://cordis.europa.eu/project/id/190185259

EU contribution	2.456.377,00 € out of 3.527.060,00 €
Coordinator	SIGHTEC ISRAEL LTD
Website:	-
Coordinator Contact	Contact the organisation
Call for proposal	HORIZON-EIC-2021-ACCELERATORCHALLENGES-01
Start Date	1 April 2022
End Date	31 December 2023

The EU-funded AUTOFLY project is intended at providing drones with situational awareness capabilities. The project is addressing the growing need for advanced situational awareness in the expanding field of drone applications, such as delivery and inspection. The project is developing a distinctive platform that empowers drones to execute complex tasks autonomously, leveraging cutting-edge algorithms for vision-based orientation, navigation, real-time detection & tracking, and autonomous inspection. The platform facilitates continuous communication and real-time analytics broadcast to mission control, utilizing minimal network bandwidth, and operates beyond line of sight and without reliance on GPS.

Sightec's system enables autonomous and remotely piloted vehicles to navigate similarly to human pilots by cross-referencing map data with visually observed landmarks, known waypoints, and visible obstacles and hazards. This innovative approach allows for the execution of tasks that are currently impossible with existing technology, as demonstrated by a successful delivery drone flight in southern Israel in February 2021, which operated beyond line-of-sight and without the use of GPS. The AUTOFLY project is a significant stride towards enhancing autonomous navigation and operational capabilities of drones in various applications.

3.3.3 ODYSSEUS

Project	ODYSSEUS
Full Title	Unobtrusive Technologies for Secure and Seamless Border Crossing for Travel Facilitation
GRANT AGREEMENT ID	101073910
Source of information	https://cordis.europa.eu/project/id/101073910
EU contribution	3.457.062,50 € out of 4.598.000,00 €
Coordinator	SOFTWARE IMAGINATION & VISION SRL
Call for proposal	HORIZON-CL3-2021-BM-01
Start Date	1 January 2023
End Date	31 December 2025

The EU-funded ODYSSEUS project aims to develop digital solutions enabling citizens to seamlessly cross borders without stopping. Different technologies, i.e. AI and advanced scanning tools (based on X-rays or unmanned aerial vehicles) will also eliminate the friction for border authorities, enabling them to remotely validate identities and check vehicles, luggage or cargos.

3.3.4 URANUS

Project	URANUS
Full Title	Real-Time Urban Mobility Management via Intelligent UAV-based Sensing
GRANT AGREEMENT ID	101088124

Source of information	https://cordis.europa.eu/project/id/101088124
EU contribution	1.999.938,00 €
Coordinator	University of Cyprus
Website	-
Call for proposal	HORIZON-ERC-2022-COG
Start Date	1 July 2023
End Date	30 June 2028

The URANUS project is addressing urban mobility inefficiencies and congestion by leveraging UAVs for real-time, dynamic, and continuous traffic sensing. Despite the potential of UAVs in capturing high-quality traffic data, their use has been limited to occasional road network surveillance. URANUS aims to utilize UAVs for real-time sensing of both vehicular and pedestrian traffic and employ the collected data for enhanced urban mobility (UM) management. The project will focus on intelligent spatiotemporal sampling from UAVs, generating comprehensive spatiotemporal measurement sets, developing methodologies for joint control of UM and UAV networks, and strategically selecting measured parameters. The framework developed by URANUS will encompass UM monitoring, UM control, and UAV operational planning methodologies. The success of URANUS could revolutionize the joint optimization between sensing, monitoring, and control in UM management and other UAV-centric applications like air pollution monitoring.

3.3.5 EGeNiouSS

Project	EGeNiouSS
Full Title	EGNSS-based Visual Localisation to enable AAA-PNT in small devices & applications
GRANT AGREEMENT ID	101082128
Source of information	https://cordis.europa.eu/project/id/101082128
EU contribution	2.999.946,00 € out of 3.407.310,25 €
Coordinator	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
Call for proposal	HORIZON-EUSPA-2021-SPACE
Start Date	1 December 2022
End Date	31 May 2026

As satellites are critical infrastructure, it is imperative that satellite-based positioning, navigation and timing (PNT) operate reliably to support dependent infrastructures such as communication, transport and energy. Interruption or manipulation of global navigation satellite systems (GNSS) signals pose a threat to safety and security. Meanwhile, augmentation systems that enhance GNSS performance can be very expensive. The goal of the EU-funded EGeNiouSS project is to improve existing European GNSS services by developing an accurate and economical cloud service that utilises novel multi-sensor navigation with a visual localisation component to compensate for common GNSS issues. Initially, an application programming interface will be integrated for smartphones and drones to demonstrate the service in three case studies. After validation, the service will be scaled and adapted for wider purposes.

3.3.6 SAFIR-Ready

Project	SAFIR-Ready
Full Title	Obtain Flight Mission Readiness, Enabling Rapid Intervention For Healthcare And Critical Infrastructure, Leveraging All Value Chain Actors And U-Space Services
GRANT AGREEMENT ID	101114855
Source of information	https://cordis.europa.eu/project/id/101114855
EU contribution	6.497.545,50 € out of 9.293.275,00 €
Coordinator	HELICUS BVBA B
Website	-
Call for proposal	HORIZON-SESAR-2022-DES-IR-01
Start Date	01/06/2023
End Date	31/05/2026

SAFIR-Ready is focused on developing advanced U-Space services, aiming to facilitate automated, time-critical drone-based services for both medical and non-medical applications. The use cases include non-medical critical missions such as inspection flights for railways and electrical grids and shore to ship transports.

The project will develop a Dynamic Capacity Management System, Detect and Avoid algorithms, and Machine to Machine communication and decision-making capabilities. The developed services will be demonstrated in Antwerp, Tartu, and Flushing, covering a variety of use cases with a base setup that includes a Command-and-Control Center and a drone agnostic Drone Cargo Port. Additionally, the project will conduct research on social acceptance, privacy protection, and environmental impact, ensuring a holistic approach to drone-based service development.

3.3.7 COVER

Project	COVER
Full Title	Cooperative And Intelligent Unmanned Aerial Vehicles For Emergency Response Applications
GRANT AGREEMENT ID	101086228
Source of information	https://cordis.europa.eu/project/id/101086228
EU contribution	579.600,00 €
Coordinator	TECHNISCHE UNIVERSITEIT EINDHOVEN
Website	-
Call for proposal	HORIZON-MSCA-2021-SE-01
Start Date	01/01/2023
End Date	31/12/2026

The EU-funded COVER project is focused on developing a cooperative, connected, and intelligent UAV system to enhance emergency response applications (ERAs) amid increasing climate change-induced threats. The project aims to create a context-aware and service-oriented UAV-to-everything network, robust cooperative UAV sensing and computing schemes, and intelligent cooperative UAV control strategies. These developments will leverage cutting-edge technologies like edge computing, cooperative sensing, intelligent control, and machine learning to address challenges in ERAs such as flooding, wildfires, and earthquakes. The project brings together a consortium of leading academic institutions and industrial partners to foster knowledge sharing, promote research innovation, and contribute to European leadership in UAVs and related technologies. The innovations from the COVER

project have the potential for broad applications, extending to areas like smart cities, public safety, and agriculture, aiming to provide efficient and faster services to save lives and reduce economic loss in emergency situations.

3.3.8 OVERWATCH

Project	OVERWATCH
Full Title	Integrated holographic management map for safety and crisis events
GRANT AGREEMENT ID	101082320
Source of information	https://cordis.europa.eu/project/id/101082320
EU contribution	2.998.934,38 € out of 3.619.906,25 €
Coordinator	ITHACA
Website	-
Call for proposal	HORIZON-EUSPA-2021-SPACE
Start Date	01/11/2022
End Date	31/10/2025

Climate change is escalating the frequency and impact of natural hazards globally, necessitating advanced planning and command tools. The EU-funded OVERWATCH project is a response to this urgent need, aiming to construct a comprehensive system for protecting citizens, land, and infrastructure. This project is set to develop an integrated holographic management system to aid in the response to, recovery from, and mitigation of emergencies and disasters. It will amalgamate EGNSS and Copernicus services with cutting-edge technologies like AI, drones, 5G, and augmented reality, enabling authorities to swiftly respond to emergencies. The objective is to create a decentralized command platform with decision support tools that can manage air, water, and ground assets and personnel efficiently. This innovative combination of technologies and services will provide a valuable resource for addressing the multifaceted challenges posed by natural disasters, aiming to minimize their devastating impacts on people, property, and the economy.

3.3.9 THRUST

Project	THRUST
Full Title	Substituting Helicopters with Climate-Friendly Fixed-Wing Drones For Infrastructure Inspection
GRANT AGREEMENT ID	101071876
Source of information	https://cordis.europa.eu/project/id/101071876
EU contribution	€ 75 000,00
Coordinator	UAB AERODIAGNOSTIKA Lithuania
Website	-
Call for proposal	HORIZON-EIE-2021-SCALEUP-01
Start Date	1 June 2022
End Date	28 February 2023

THRUST is aimed at developing inspecting infrastructure with climate-friendly drones. In EU total length of overhead electricity lines reaches 5.3 million km requiring regular inspections, traditionally conducted using helicopters, which emit substantial amounts of greenhouse gases. Addressing this environmental concern, the EU-funded THRUST project is innovating greener monitoring solutions by developing a fleet of UAVs or drones, fortified with LiDAR, visible light, and thermal cameras. These advanced drones, designed to inspect up to 300 km of lines daily, integrate machine learning to detect

faults in the grid swiftly and accurately, offering an eco-friendlier and more efficient alternative to helicopters and walking crews. The implementation of these drones is projected to significantly reduce CO2 emissions, potentially saving 1.2 million tonnes of CO2 annually in the EU.

Additionally, THRUST is leveraging the Women TechEU initiative to foster female participation in the aviation industry, aiming to inspire more women to join this sector. The project aspires to position THRUST as a leading deep-tech start-up in drone-based infrastructure inspections, emphasizing women's involvement and aiming to scale its innovative solutions, thereby contributing to environmental conservation and gender diversity in aviation.

3.3.10 EMERITUS

Project	EMERITUS
Full Title	Environmental Crimes' Intelligence And Investigation Protocol Based On Multiple Data Sources
GRANT AGREEMENT ID	101073874
Source of information	https://cordis.europa.eu/project/id/101073874
EU contribution	4.634.193,75 € out of 5.525.062,50 €
Coordinator	GMV AEROSPACE AND DEFENCE SA
Call for proposal	HORIZON-CL3-2021-FCT-01
Start Date	1 September 2022
End Date	31 August 2025

Addressing the escalating concern of environmental crime, the EU-funded EMERITUS project is innovating a comprehensive investigation protocol, utilizing advanced technologies like drones and satellite data, to aid police and border guards in environmental protection. The project is a collaborative effort involving authorities from five countries, security experts, training specialists, and technological partners, aiming to develop a geo-intelligence platform. This platform will integrate various monitoring and analysis technologies to provide a unified view of relevant data and information, supporting decision-making processes in environmental crime investigations.

The EMERITUS project is also focused on creating a training programme, blending theoretical knowledge with practical simulations, to enable end users to effectively leverage the platform for environmental crime investigation and prevention. The co-created investigation protocol and the platform will undergo validation through simulations based on realistic use cases, aiming to refine the approach and provide evidence-based recommendations for policy authorities and decision-makers. The initiative is a significant step towards enhancing the capabilities of enforcement authorities in combating environmental crimes and fostering ecosystem preservation.

3.3.11 HAIKU

Project	HAIKU
Full Title	Human AI teaming Knowledge and Understanding for aviation safety
GRANT AGREEMENT ID	101075332
Source of information	https://cordis.europa.eu/project/id/101075332
EU contribution	5.778.938,63 € out of 8.181.687,50 €
Coordinator	DEEP BLUE SRL
Website	https://haikuproject.eu/

Call for proposal	HORIZON-CL5-2021-D6-01
Start Date	1 September 2022
End Date	31 August 2025

The EU-funded HAIKU project is at the forefront of integrating AI in aviation, focusing on developing AI Digital Assistants tailored for various aviation segments including commercial pilots, urban air mobility, remotely piloted drones, and air traffic controllers. The project is poised to deliver prototypes that will explore Human-AI Teaming through interactive models, aiming to enhance safety and operational efficiency in the aviation sector.

HAIKU is committed to addressing crucial research questions concerning the optimal human-AI relationship, the explainability and trustworthiness of AI in aviation applications, and the methodologies for effective human-in-the-loop AI learning. The project will yield new Human Factors design guidance ('HF4AI' Capabilities) and methods, ensuring the development of safe, effective, and trustworthy Digital Assistants for Aviation. It will also provide a series of use cases illustrating the diverse roles and tasks of the Digital Assistant in various scenarios, contributing to the development of new safety and validation assurance methods.

HAIKU is focused on continuous engagement with stakeholders, including policy makers and professional associations, to formulate guidance on socially acceptable AI in safety-critical operations. The project aspires to maintain aviation's strong safety culture record while facilitating the early integration of Digital Assistants into aviation systems, ensuring that future autonomous AI systems align with human judgments and decisions, thereby reinforcing aviation safety and societal acceptance.

3.3.12 MAGDA

Project	MAGDA
Full Title	Meteorological Assimilation from Galileo and Drones for Agriculture
GRANT AGREEMENT ID	101082189
Source of information	https://cordis.europa.eu/project/id/101082189
EU contribution	1.705.231,00 € out of 2.059.062,50 €
Coordinator	GEOMATICS RESEARCH & DEVELOPMENT SRL
Call for proposal	HORIZON-EUSPA-2021-SPACE
Start Date	1 November 2022
End Date	30 April 2025

Reliable weather prediction and efficient irrigation practices are essential for modern agriculture. Advanced technology such as the GNSS and drones allow precise atmosphere monitoring. The EU-funded MAGDA project will develop a toolchain for atmosphere monitoring and weather forecasting, and an exact weather/irrigation/crop monitoring advisory, with GNSS (including Galileo) at its core to deliver valuable information to agricultural operators. The project will exploit the potential of assimilating GNSS-derived, drone-derived and Copernicus EO-derived data sets to improve the prediction of severe weather events and weather-driven agriculture pests and diseases. The improved weather forecast will in turn drive a hydrological model for irrigation performance and water accounting.

3.4 Update about research projects on disinformation

In the last decade the European Commission called for and funded a great number of research and development projects about disinformation and Foreign Information Manipulation and Influence (FIMI) [38].

Horizon 2020 mobilised significant resources in addressing information veracity for social media and media. The Social Observatory for Disinformation and Social Media Analysis (SOMA [39]) along with other EU-funded projects (PROVENANCE [40], SocialTruth [41], EUNOMIA [42], WeVerify [43]) provided a springboard for the social media sector to steer an understanding of its dynamics and the relationship between social media and other sectors. Other projects adjusted their activities and included coronavirus-related disinformation in scope, such as Co-Inform [44], QUEST [45] and TRESCA [46].

The aim of the Horizon2020 funded FANDANGO [47] project is to aggregate and verify different typologies of news data, media sources, social media, open data, so as to detect fake news and provide a more efficient and verified communication for all European citizens. Projects MISTRUST [48] and RADICALISATION [49] also contributed to the fight of propaganda, disinformation campaigns and misinformation.

The European Research Council (ERC) also supports theoretical investigations like those carried out by projects COMPROP [50], DEBUNKER [51], and the ongoing project FARE [52]. The ERC also supported proof of concept projects like GoodNews [53], which applied deep learning technology for the detection of fake news.

The European Innovation Council supported companies in developing semi-automated fake-news detection systems through actions like TRUTHCHECK [54] and NEWTRAL [55]. It also organized the #EUvsVirus Hackathon and the "Matchathon" with challenges on the mitigating fake news spreading [56].

The Joint Research Centre (JRC) developed a machine-learning program, called Misinfo Classifier [57], to identify patterns in the language, notably the "shrillness" of language, and identify whether something might be fake news or not.

The European Digital Media Observatory (EDMO) [58] is a project that supports the independent community working to combat disinformation.

In Horizon Europe, the current research and innovation framework programme, a variety of projects was funded in the area of disinformation fighting: AI4TRUST [59], TITAN [60], vera.ai [61], FERMI [62], VIGILANT [63], DisAI [64], and FARE_AUDIT [65]. In the calls for proposals for 2023, there was a specific call about "Through AI from Disinformation to Trust" but the winners are not known yet.

The DG CNECT (Directorate-General Communications NEtworks, Content and Technology) funded the NODES [66] project that will create the first European Narrative Observatory based on the analysis of narratives to tackle disinformation within the public sphere working in four languages (English, French, Spanish and Polish) and focusing on Climate Change, Migration and Covid-19.

In 2022 the European Commission published a call for proposal titled "Cyber and information warfare toolbox" within the European Defence Fund [67] with the specific objective of countering threats posed by new and evolving cyber and hybrid tools (e.g., disinformation, deep fakes) which are fully part of Cyber and Information Warfare. The call was won by a consortium led by Leonardo (Italy) with a total estimated costs of more than 41 million euros [68].

In this frame, the European Media and Information Fund (EMIF) launched new calls for proposals to fight disinformation in 2023 [69].

Table 5 Selected projects funded in H2020, Horizon Europe and EDF, and by the ERC and EIC on disinformation

Acronym	Title	Start-end year
EUCINF	European Cyber and INFormation warfare toolbox	2023 – 2026
AI4TRUST	AI-based-technologies for trustworthy solutions against disinformation	2023 – 2026
NODES	Narratives Observatory combatting Disinformation in Europe Systemically	2022 - 2023
TITAN	AI for Citizen Intelligent Coaching against Disinformation	2022 – 2025
vera.ai	VERification Assisted by Artificial Intelligence	2022 – 2025
FERMI	Fake nEws Risk MItigator	2022 – 2025
VIGILANT	Vital IntelliGence to Investigate ILlegAl DisiNformaTion	2022 – 2025
DisAI	Improving scientific excellence and creativity in combating disinformation with artificial intelligence and language technologies	2022 – 2025
FARE_AUDIT	Fake News Recommendations - an Auditing System of Differential Tracking and Search Engine Results	2022 – 2024
FARE	Fake news and real people – using big data to understand human behaviour	2020 – 2025
RADICALISATION	We're not neo-Nazis anymore': Radicalisation strategies in online far-right propaganda and disinformation campaigns	2020 – 2023
MISTRUST	Correcting misinformation: The role of source (un)trustworthiness on the effects of repetition and contradiction in judgments of information's truth-value	2020 – 2022
TRESCA	Trustworthy, Reliable and Engaging Scientific Communication Approaches	2020 – 2022
QUEST	QUality and Effectiveness in Science and Technology communication	2019 – 2021
TRUTHCHECK	Fake News Recognition applying Service-based Cross-Media Analytics	2019
NEWTRAL	First real-time fact-checking tool to fight against the fake news and disinformation	2019
PROVENANCE	Providing Verification Assistance for New Content	2018 – 2022
FANDANGO	FAke News discovery and propagation from big Data ANalysis and artificial intelliGence Operations	2018 – 2021
Co-Inform	Co-Creating Misinformation-Resilient Societies	2018 – 2021
SOMA	Social Observatory for Disinformation and Social Media Analysis	2018 – 2021
WeVerify	Wider and enhanced verification for you	2018 – 2021
SocialTruth	Open Distributed Digital Content Verification for Hyper-connected Sociality	2018 – 2021
EUNOMIA	User-oriented, secure, trustful & decentralised social media	2018 – 2021

GoodNews	Fake news detection in social networks using geometric deep learning	2018 – 2020
COMPROP	Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe	2016 – 2020

4. Main findings

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

Joint use of SDN and Blockchain technology

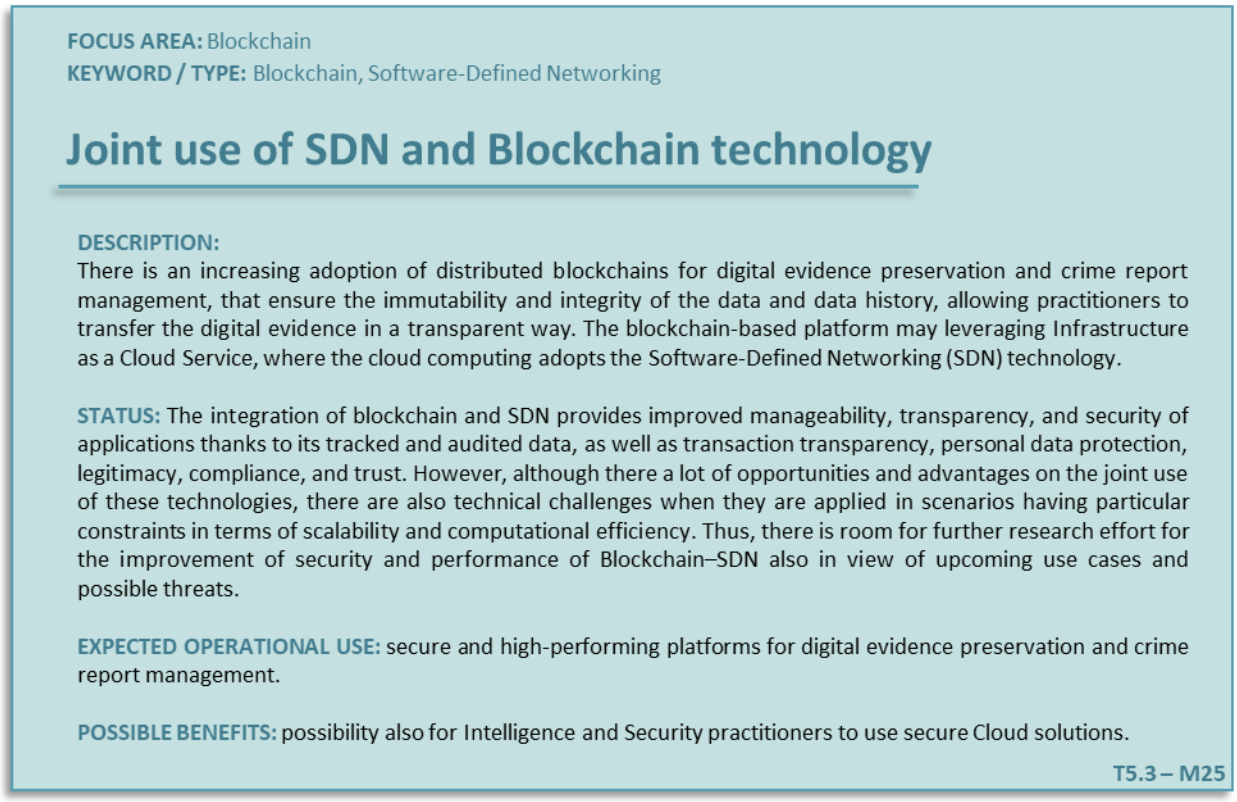

Figure 2 Main results: Joint use of SDN and Blockchain technology

Secure and high-performing platforms for digital evidence preservation and crime report management can be blockchain-based platforms leveraging Infrastructure as a Cloud Service, where the cloud computing adopts the SDN technology.

This can provide benefit, but also new threats which need further research before implementation of this solution. NOTIONES will monitor the evolution of this technology in the upcoming years.

Spectral search and discovery tool

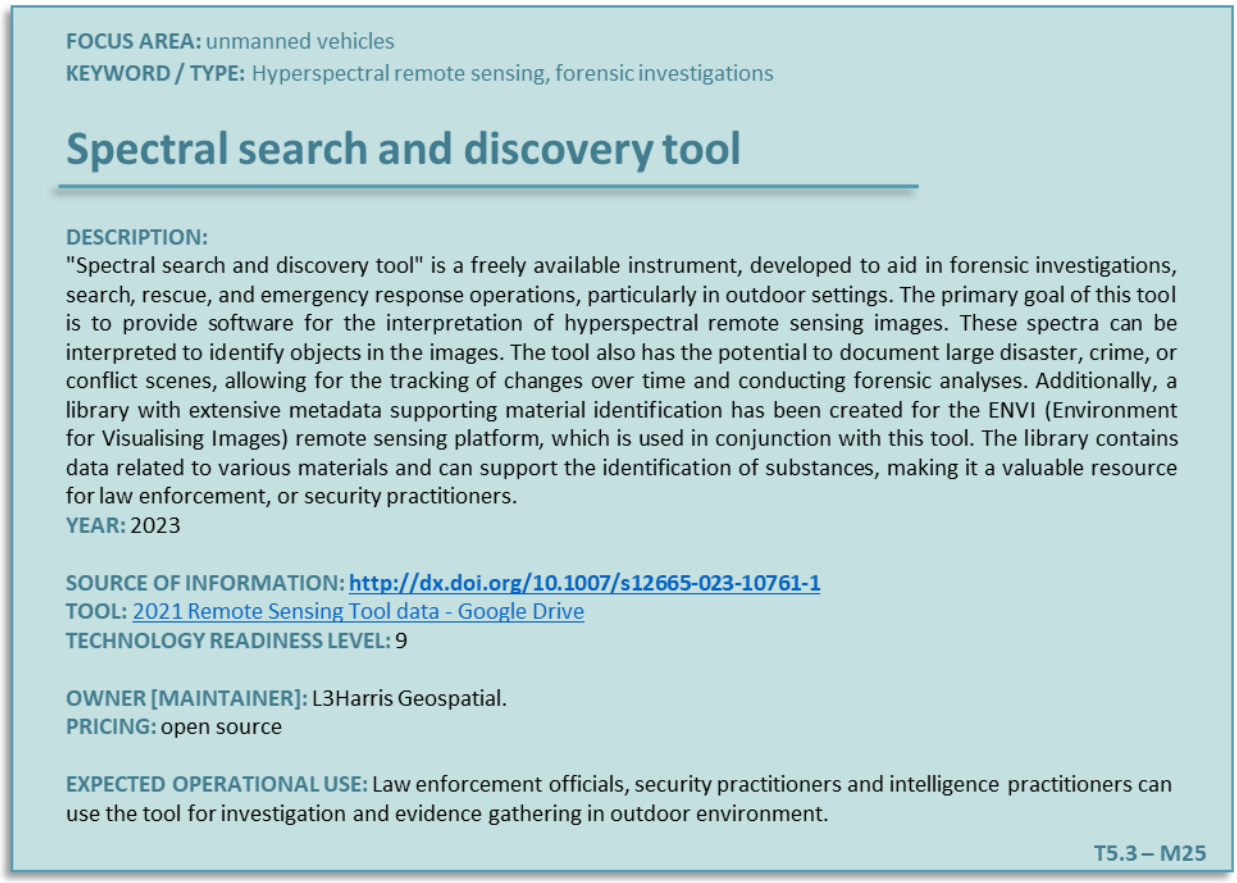

Figure 3 Main results: Spectral search and discovery tool

This innovative tool, developed by L3Harris Geospatial serves as a versatile search and discovery instrument for both forensic investigations and emergency response operations. It is made accessible to the forensic community and other interested scientists free of charge, thus facilitating extensive academic applications, applied hyperspectral imaging, and reflective spectroscopy investigations. The tool encompasses a comprehensive dataset comprising human, geologic, and environmental materials, making it a valuable resource for fundamental research, applied research, and practical operations conducted by law enforcement and various organizations. Its applications are diverse, with the primary intent being the interpretation of hyperspectral images in outdoor settings, extending to the documentation of disasters, emergencies, investigations related to violence, and hostage-taking scenarios. Additionally, it has the potential to contribute to the investigation and identification of hostages in international settings by providing exemplars and analogs of relevant materials. The tool's value lies in its capacity to assist law enforcement, emergency management, and a wide range of agencies and organizations in their respective missions and endeavors.

AUTOFLY project

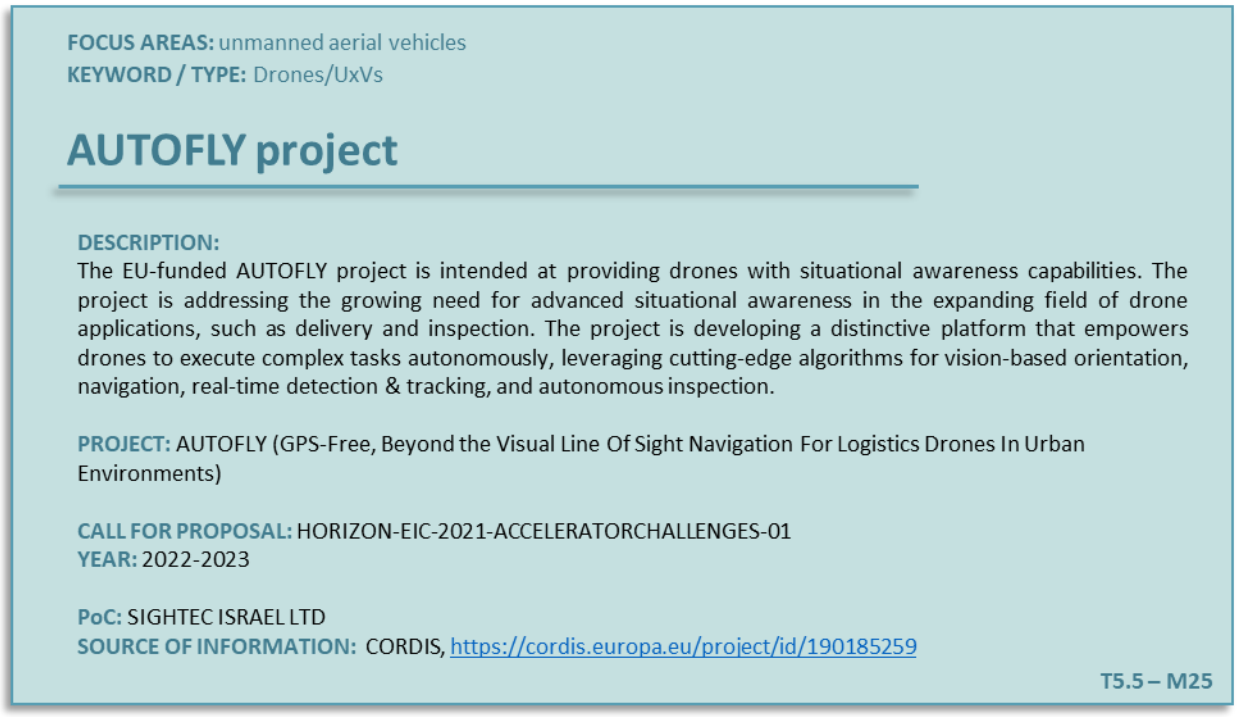

Figure 4 Main findings - AUTOFLY project

The EU-funded AUTOFLY project aims to equip drones with advanced situational awareness. It's developing a unique platform for autonomous drone operations using cutting-edge vision-based algorithms, enabling real-time detection and tracking, navigation, and inspection. This technology allows drones to operate autonomously, beyond line of sight, and without relying on GPS, opening up new possibilities for various applications. This project represents a significant step in advancing drone autonomy.

SAFIR-Ready project

Figure 5 Main findings - SAFIR-Ready project

SAFIR-Ready creates U-Space services with a central Command and Control Center and automated ground integration for urgent drone-based medical and non-medical missions, including infrastructure inspections and shore-to-ship transport. It covers various regions and addresses social acceptance, privacy, and environmental concerns. This project is of interest to security and intelligence practitioners as it develops advanced capabilities for autonomous drones, enhancing surveillance and critical cargo transport, which can aid in intelligence gathering and security operations.

5. Conclusions and next steps

This document represents the product of the fourth run of tasks T5.2 and T5.3 of WP5, which performed the research monitoring activities during months M25 and M26 (September, October 2023).

Task T5.2 performed the horizon scanning activity through exploratory research on the online scholar and patent database The Lens and the open web, on two topics:

- drones/unmanned vehicles: legal aspects, defence applications, use for crime detection and forensic, use for surveillance, tracking, patrolling, detection;
- blockchain solutions: digital evidence preservation and crime report management.

Task T5.3 performed the monitoring of EU-funded research projects on the CORDIS database on the following topics: drones/unmanned vehicles (12 projects), blockchain solutions (9 projects + 3), and tools for privacy-enhancing processing of data (10 projects).

WP5 also performed the update about research projects on disinformation.

In conclusion, the results of the fourth run of tasks T5.2 and T5.3 were documented in this report. The main findings are summarised in section 43.4, highlighting technologies and EU projects that are most promising for the purposes of NOTIONES:

- joint use of SDN and Blockchain technology;
- spectral search and discovery tool;
- Autofly project;
- SAFIR-Ready project.

With regard to the next steps, two main actions are foreseen in the next runs of tasks T5.2 and T5.3 in months M31-M32:

- The research of T5.2 will be repeated on CORDIS with updated search parameters;
- 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 D5.6 "*Monitoring of EU Research and Horizon Scanning -v5*", due in M32.

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] S. Mehta, K. S. Kumari, P. Jain, H. Raikwar and S. Gor, "Blockchain driven Evidence Management System," *2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP),* 2023.

[4] Ethereum, [Online]. Available: https://ethereum.org/en/. [Accessed 3 October 2023].

[5] C. Shilpa and A. H. Shanthakumara, "An Implementation of Blockchain Technology in Combination with IPFS for Crime Evidence Management System," *2023 International Conference on Computer Communication and Informatics (ICCCI),* 2023.

[6] S. Verma, A. Kumar, S. Pandey and P. Negi, "Blockchain and Cloud Computing used in Preservation of Crime Scene Evidences," *2023 2nd International Conference on Edge Computing and Applications (ICECAA),* 2023.

[7] S. Shetty, K. Shinde, D. Shelke, R. Garje and P. A. Mahtre, "Crime Evidence Over Blockchain," *International Journal of scientific research in engineering and management,* vol. 7, no. 4, 2023.

[8] R. Amin, R. A. Chowdhury, S. M. Tanjim, A. Islam and M. S. Islam, "xCRM: Blockchain Interoperable Crime Report Management System By Utilizing Hyperledger Cacti & Private Data Collection (PDC)," *2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM),* 2023.

[9] Hyperledger Foundation, "Cacti," [Online]. Available: https://www.hyperledger.org/projects/cacti. [Accessed 3 October 2023].

[10] A. Karambe, "Blockchain-Based Approach for Tracking Global Criminals," *International Journal of scientific research in engineering and management,* vol. 7, 2023.

[11] S. Sonkamble, A. Kadu, P. Ghorpade, O. Ingule and V. Dhage, "Criminal Records and Reporting System," *International Journal for Research in Applied Science and Engineering Technology,* vol. 11, no. 5, pp. 6736-6743.

[12] R. Bhalerao, A. Prabhu and S. Banerjee, "Block Crime: Criminal Incidence Detection Using Facial Recognition Based on Concepts of Blockchain," in *Proceedings of International Conference on Data Analytics and Insights, ICDAI 2023*, 2023, pp. 791-803.

[13] Truffle Suite, "Ganache," [Online]. Available: https://trufflesuite.com/ganache/. [Accessed 29 September 2023].

[14] Open CV, "Open Computer Vision Library," [Online]. Available: https://opencv.org/. [Accessed 3 October 2023].

[15] Indian Government, "National Crime Records Bureau," [Online]. Available: https://ncrb.gov.in/. [Accessed 29 September 2023].

[16] N. K. Rathore, Y. Khan, S. Kumar, P. Singh and S. Varma, "An evolutionary algorithmic framework cloud based evidence collection architecture," *Multimedia Tools and Applications,* 2023.

[17] Y. Zhuang, Z. Liu, P. Qian, Q. Liu, X. Wang and Q. He, "Smart Contract Vulnerability Detection Using Graph Neural Networks," *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20),* 2020.

[18] A. Rahman, A. Montieri, D. Kundu, M. R. Karim, M. J. Islam, S. Umme, A. Nascita and A. Pescapé, "On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives," *Journal of Network and Systems Management,* vol. 30, no. 73, 2022.

[19] O. S. Abuomar and R. Yale Gross, "Using Blockchain, RAID, & BitTorrent Technologies to Secure Digital Evidence from Ransomware," *2023 IEEE International Conference on Electro Information Technology (eIT),* 2023.

[20] P. Akello, N. Vemprala, N. Lang Beebe and K.-K. R. Choo, "Blockchain Use Case in Ballistics and Crime Gun Tracing and Intelligence: Toward Overcoming Gun Violence," *ACM Transactions on Management Information Systems,* vol. 14, no. 1, pp. 1-26, 2023.

[21] V. Lappas, H.-S. Shin, A. Tsourdos, D. Lindgren, S. Bertrand, J. Marzat, H. Piet-Lahanier, Y. Daramouskas and V. Kostopoulos, "Autonomous Unmanned Heterogeneous Vehicles for Persistent Monitoring," *Drones 2022,* vol. 6, no. 4, 2022.

[22] S. Matalonga, S. White, J. Hartmann and e. al., "A Review of the Legal, Regulatory and Practical Aspects Needed to Unlock Autonomous Beyond Visual Line of Sight Unmanned Aircraft Systems Operations," *J Intell Robot Syst,* vol. 106, no. 10, 2022.

[23] D. Tychyna, k. A. Antoshchu and R. Pertsev, "Forensic support for the use of an unmanned aerial vehicle (drone) in a pre-trial investigation," *Науковий вісник Ужгородського Національного Університету,* vol. 78, no. 2, p. 7, 2023.

[24] N. Mohd Sabri, M. Chainchel Singh, M. Mahmood, L. S. Khoo, M. Y. P. M. Yusof, C. C. Heo, M. D. M. M. Nasir and H. Nawawi, "A scoping review on drone technology applications in forensic science," *SN Applied sciences,* vol. 5, no. 233, 2023.

[25] M. Krekeler, M. Burke, S. Allen and e. al., "A novel hyperspectrical remote sensing tool for detecting and analyzing human materials in the environment: a geoenvironmental approach to aid in emergency response," *Environmental Earth Sciences,* 2023.

[26] A. Georgiou, P. Masters, S. Johnson and L. Feetham, "UAV-assisted real-time evidence detection in outdoor crime scene investigations," *Journal of forensic sciences,* 2022.

[27] H. Sachdeva, S. Gupta, A. Misra, K. Chauhan and M. Dave, "Improving Privacy and Security in Unmanned aerial vehicles network using blockchain," *Int. J. of Communication Networks and Distributed Systems (IJCNDS) 2023,* p. 21, 2023.

[28] A. Ingale, M. Vispute, S. Sonawane, H. Guthula and P. D. R. Iyer, "Hawk Eye Unmanned Aerial Vehicle for monitoring," *International journal for research ,* vol. 10, no. 5, p. 7, 2022.

[29] Z. Zhang, W. Ouyang, H. Gao and X. Jing, "Edge UAV Detection Based on Cyclic Spectral Feature: An intelligent scheme," *Hindawi; Wireless Communications and Mobile Computing,* p. 8, 2022.

[30] A. Tullu, M. Hassanalian and H.-Y. Hwang, "Design and Implementation of Sensor Platform for UAV-Based Target Tracking and Obstacle Avoidance," *Drones 2022,* vol. 6, no. 89, 2022.

[31] G. Liu, L. Shu, Y. Yang and C. Jin, "Unsupervised video anomaly detection in UAVs: a new approach based on learning and inference," *frontiers in sustainable cities,* vol. 5, p. 13, 2023.

[32] R. Sugano, R. Shinkuma, T. Nishio, S. Itahara and N. B. Mandayam, "Watch from sky: machine-learning-based multi-UAV network for predictive police surveillance," *cornell university,* 2022.

[33] M. Watney, "Ethical and Legal Aspects Pertaining to law Enforcement use of drones," *Proceedings of the 17th International Conference on Information Warfare and Security,* p. 8, 2022.

[34] Siong, "Usage of drones by law enforcement in daily duties: legal issues in Malaysia," *International journal of law, goverment and communication,* vol. 7, no. 29, p. 9, 2022.

[35] V. S. Tulinov, I. V. Bilykh, O. M. Merdova, O. O. Volobuieva and M. Veselov, "Activities of Law Enforcement Agencies in the context of the introduction of innovative technologies (comparative legal aspect)," *CUESTIONES POLÍTICAS ,* vol. 40, no. 72, pp. 145-163, 2022.

[36] M. Osiecki, A. Fortońska, M. Berus and M. Włodarczyk, "Drone as a target of a terrorist attack and a weapon againast terrorism - analysis in the light of the international law," *Journal of Intelligent & Robotic Systems,* 2022.

[37] I. Yefimenko, "Modern possibilities of using unmanned aerial vehicles by Police authorities and units: analysis of foreign and ukrainian experience," *Scientific journal of national academy of international affairs,* vol. 27, no. 3, pp. 65-77, 2022.

[38] European Commission, "Funded projects in the fight against disinformation," [Online]. Available: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_en.

[39] CORDIS, "SOMA," [Online]. Available: https://cordis.europa.eu/project/id/825469.

[40] CORDIS, "PROVENANCE," [Online]. Available: https://cordis.europa.eu/project/id/825227.

[41] CORDIS, "SocialTruth," [Online]. Available: https://cordis.europa.eu/project/id/825477.

[42] CORDIS, "EUNOMIA," [Online]. Available: https://cordis.europa.eu/project/id/825171.

[43] CORDIS, "WeVerify," [Online]. Available: https://cordis.europa.eu/project/id/825297.

[44] CORDIS, "Co-Inform," [Online]. Available: https://cordis.europa.eu/project/id/770302.

[45] CORDIS, "QUEST," [Online]. Available: https://cordis.europa.eu/project/id/824634.

[46] CORDIS, "TRESCA," [Online]. Available: https://cordis.europa.eu/project/id/872855.

[47] CORDIS, "FANDANGO," [Online]. Available: https://cordis.europa.eu/project/id/780355.

[48] CORDIS, “MISTRUST,” [Online]. Available: https://cordis.europa.eu/project/id/844296.

[49] CORDIS, “RADICALISATION,” [Online]. Available: https://cordis.europa.eu/project/id/845643.

[50] CORDIS, “COMPROP,” [Online]. Available: https://cordis.europa.eu/project/id/648311/en.

[51] CORDIS, “DEBUNKER,” [Online]. Available: https://cordis.europa.eu/project/id/682758.

[52] CORDIS, “FARE,” [Online]. Available: https://cordis.europa.eu/project/id/853566.

[53] CORDIS, “GoodNews,” [Online]. Available: https://cordis.europa.eu/project/id/812672.

[54] CORDIS, “TRUTHCHECK,” [Online]. Available: https://cordis.europa.eu/project/id/854497.

[55] CORDIS, “NEWTRAL,” [Online]. Available: First real-time fact-checking tool to fight against the fake news and disinformation.

[56] European Commission, “European Commission #EUvsVirus Matchathon to boost the scaling up of creative solutions to Covid-19 challenges,” [Online]. Available: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/european-commission-euvsvirus-matchathon-boost-scaling-creative-solutions-covid-19-challenges-2020-05-20_en.

[57] European Commission, “JRC to release AI tech for coronavirus fact-checkers,” [Online]. Available: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/jrc-release-ai-tech-coronavirus-fact-checkers-2020-06-10_en.

[58] EDMO, “European Digital Media Observatory,” [Online]. Available: https://edmo.eu/.

[59] CORDIS, “AI4TRUST,” [Online]. Available: https://cordis.europa.eu/project/id/101070190.

[60] CORDIS, “TITAN,” [Online]. Available: https://cordis.europa.eu/project/id/101070658.

[61] CORDIS, “vera.ai,” [Online]. Available: https://cordis.europa.eu/project/id/101070093.

[62] CORDIS, “FERMI,” [Online]. Available: https://cordis.europa.eu/project/id/101073980.

[63] CORDIS, “VIGILANT,” [Online]. Available: https://cordis.europa.eu/project/id/101073921.

[64] CORDIS, “DisAI,” [Online]. Available: https://cordis.europa.eu/project/id/101079164.

[65] CORDIS, “FARE_AUDIT,” [Online]. Available: https://cordis.europa.eu/project/id/101100653.

[66] NODES, “Narratives Observatory combatting Disinformation in Europe Systemically,” [Online]. Available: https://nodes.eu/.

[67] European Defence Fund calls 2022, “Cyber and information warfare toolbox,” 2022. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2022-da-cyber-ciwt.

[68] EDF, “EUCINF factsheet,” 2022. [Online]. Available: https://defence-industry-space.ec.europa.eu/document/download/abca2b84-bbba-409c-958d-a0767637b76a_en?filename=EUCINF%20-%20Factsheet_EDF22.pdf.

[69] EMIF, “European Media and Information Fund launches new calls for proposals,” [Online]. Available: https://www.eui.eu/news-hub?id=european-media-and-information-fund-launches-new-calls-for-proposals.

[70] EC, “Horizon-IA HORIZON Innovation Actions,” [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-fct-01-06;callCode=null;freeTextSearchKeyword=;matchWholeText=false;typeCodes=1,2,8;statusCodes=31094501,31094502;programmePeriod=2021%20-%2.