This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293

IMMERSE. INTERACT. INVESTIGATE

INFINITY

D6.1 Recommendation report for integrating AI into LEA environments

PUBLIC [PU]

D6.1 Recommendation report for integrating AI into LEA environments

PROJECT INFORMATION

Grant Agreement No	883293
Acronym	INFINITY
Name	IMMERSE. INTERACT. INVESTIGATE
Topic	SU-FCT-02-2018-2019-2020
Funding Scheme	Research and Innovation Action
Start Date	01/06/2020
Duration	36 months
Coordinator	Airbus Defence and Space SAS

DELIVERABLE INFORMATION

Work Package	WP6 AI investigative assistant and analysis	
Deliverable	D6.1 Recommendation report for integrating AI into LEA environments	
Contractual Delivery Date	30/11/2020	
Actual Delivery Date	27/10/2021	
Type	R - Report / O - Other	
Dissemination Level	Public [PU]	
Lead Beneficiary	CERTH, VICOM	
Main Author (s)	Author Name	Organisation
	Jan Lukas Bruse	VICOM
	Stefano Masneri	VICOM

	Theodora Tsikrika	CERTH
Contributing Author (s)	Author Name	Organisation
	Alain Pagani	DFKI
	Rodolphe Roques-Couchot	EUROPOL
	Silvia Alba Uribe Mayoral	UPM
	Weidong Yang	KINEVIZ
	Christos Voulgaris	KEMEA

Reviewers	Reviewer Name	Organisation	Date
	María López de Andrés	GUCI	18/10/2021
	Rania Theodosiadou	CERTH	20/10/2021
	James Fenwick	CENTRIC	26/10/2021

REVISION HISTORY

Version	Author Name(s)	Date	Revisions
0.1	Jan Lukas Bruse	21/09/2020	First version
0.2	Stefano Masneri	23/09/2020	Revision
0.3	Jan Lukas Bruse	13/11/2020	Integration of first feedback
0.4	Jan Lukas Bruse	20/11/2020	Integration of second feedback

0.5	Jan Lukas Bruse	21/11/2020 - 24/11/2020	Preparation of final CO document
0.6	Sergio Cabrero Barros	26/11/2020	Revision
0.7	Jan Lukas Bruse	27/11/2020	Finalise CO document
0.8	Jan Lukas Bruse	25/08/2021	Draft for public release
0.9	Sergio Cabrero Barros	07/10/2021	Revision
1.0	María López de Andrés	18/10/2021	Revision
1.1	Rania Theodosiadou	20/10/2021	Revision
1.2	James Fenwick	26/10/2021	Revision
1.3	Jan Lukas Bruse	26/10/2021	Final version

EXECUTIVE SUMMARY

The INFINITY project aims to create an integrated, interactive and collaborative as well as immersive data analysis and visualisation platform, designed to assist analysts and investigators in extracting case-relevant information in cyber-attack and counter terrorism scenarios. While data visualisation and augmented and virtual reality (AR and VR) workspaces will be explored and developed in Work Package 7 (WP7, "Visualisation and Reporting"), **WP6** focusses on the development and integration of tools that leverage recent advances in the field of artificial intelligence (AI) and machine learning (ML). AI and ML techniques allow mining incoming data in order to detect unknown trends and patterns as well as predict and classify or categorise a multitude of data formats (text, sound, images, video, phone records, social network data, financial data etc.). The objective is to extract relevant, novel information that may help investigators find or track suspects and criminal networks or predict potential targets, for example.

This deliverable **D6.1** is the result of task **T6.1** "Analysis of investigative practices for AI integration", running from month 1 to month 6 of the project. The partners responsible for D6.1 are VICOM and CERTH. Contributing partners are DFKI, KEMEA, KINEVIZ, UPM, EUROPOL and for chapter 5 ENG, as they lead another AI-related task (T6.5).

The key objective of D6.1 is to identify investigative tools, methods, and capabilities which could be undertaken by AI-based tasks within INFINITY. Those tasks are **T5.2** and tasks **T6.3 - T6.6**. To this end, D6.1 provides a **guideline for future AI-related developments** in those aforementioned tasks and details a range of AI applications as desired by LEAs (chapter 3), a list of AI-based tools suggested by technical partners (chapter 4) and joins those two lists into a **proposed set of AI toolboxes** (chapter 5). For each toolbox, potential modules as well as relevance for INFINITY use cases and potential data sources, AI and ML techniques and available benchmarks are listed wherever possible.

All partners were then asked to evaluate each toolbox with respect to their respective know-how required to develop a toolbox, potential data availability and overall estimated feasibility given the remaining time and resources within INFINITY (chapter 5). Based on this scoring, a final evaluation and recommendation of relevant and feasible toolboxes is given (chapter 6), which shall serve as a guideline for further development in tasks T5.2 and T6.3 - T6.6. Chapter 7 summarises the results and outlines future steps.

The core contributions of this deliverable are:

- A brief overview of INFINITY use cases and potential applications of AI for each use case
- A detailed "wish list" of AI applications proposed by LEAs
- A list and description of AI-based tools proposed by technical partners
- A proposed set of seven "AI toolboxes" which were derived based on the previous lists and suggestions provided by LEAs and technical partners
- A brief evaluation of each toolbox provided by each partner with respect to know-how, data availability and overall estimated feasibility within INFINITY given the remaining time and resources
- A final recommendation of AI toolboxes and classification into "highly feasible", "feasible" and "not ready for development", indicating a set of tools that may potentially be developed in subsequent INFINITY tasks
- Recommendations how to address development for toolboxes that were ranked as "not ready for development"
- Provision of concrete partner names that may provide technical know-how or training data for each toolbox.

ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
BiLSTM	Bi-directional (recurrent) Long Short-Term Memory networks
CCTV	Closed-circuit Television
EC	European Commission
GDELT	Global Data on Events, Location and Tone
GTD	Global Terrorism Database
HMD	Head Mounted Display
I^3CE	Investigative Immersive and Interactive Collaboration Environment
IP	Internet Protocol (address)
LEAs	Law Enforcement Agencies
ML	Machine Learning
MR	Mixed Reality
MS	Member State
N/A, -	Not applicable, no answer provided
NLP	Natural Language Processing
OSINT	Open Source Intelligence
POI	Point of Interest
ROI	Region of Interest
SNA	Social Network Analysis
UC	INFINITY Use Case
VIA	Virtual Investigative Assistant
VR	Virtual Reality
XR	eXtended Reality

TABLE OF CONTENTS

Contents

LIST OF FIGURES

No table of figures entries found.

1 INTRODUCTION

1.1 OVERVIEW AND INFINITY CONCEPT AND APPROACH

INFINITY aims to develop a novel, digital investigation platform for law enforcement agencies (LEAs), which enables quick processing, filtering, analysis and visualisation of the various data streams an investigator or analyst faces during an investigation. Typical case-relevant data consists of images, videos, text or audio recordings scraped from the internet, the news, social media and social networks or provided by surveillance equipment as well as financial data, phone records or records related to crypto-currency networks, blogs, forums or dark nets and markets. In order to facilitate quick extraction, comprehension and sharing of relevant information, INFINITY leverages an immersive concept based on using advanced visualisation techniques combined with virtual and augmented reality (VR and AR), creating a virtual, collaborative space for investigators working from different sites together on one case. Critical information – prior to visualising – though needs to be filtered, categorised and aggregated via state-of-the-art techniques from the field of artificial intelligence (AI) and machine learning (ML). Deliverable D6.1 is constituted by this report, which will recommend concrete applications of AI within INFINITY based on requirements posed by INFINITY's use cases, feedback given by LEAs and suggestions provided by technical partners.

1.2 DELIVERABLE POSITIONING

Deliverable D6.1 is the result of task T6.1 "Analysis of investigative practices for AI integration", led by CERTH and including DFKI, KEMEA, KINEVIZ, UPM, EUROPOL and VICOM as partners. T6.1 is part of work package 6 (WP6, "AI investigative assistant and analysis"); it started in month 1 of the project and finished in month 6. WP6 generally focusses on the development of AI or ML techniques and modules that will be used to detect patterns, trends, clusters or hidden relationships as well as categorise the data processed and ingested by modules developed in WP5 ("Data acquisition, ingestion and processing"). The specific INFINITY tasks directly related to developing modules applying AI or ML techniques are:

- → **T5.1** developing automated query reformulation mechanisms
- → **T5.2** focussed on object and activity detection and recognition
- → **T6.3** focussed on event and trend detection
- → **T6.4** focussed on graph analysis and recommendation, and social network analysis
- → **T6.5** focussed on pattern recognition in graphs
- → **T6.6** developing the INFINITY *Virtual Investigative Assistant* (VIA); a recommender system learning user behaviour and providing alarms.

For those tasks, concrete AI applications to be addressed have not been defined in detail, which is why D6.1 aims to detect which applications may be relevant and feasible within INFINITY, thereby providing a guideline for future development within those tasks. As INFINITY will provide a virtual, immersive platform visualising case-relevant information in an interactive manner, outputs from the aforementioned AI-related tasks will likely be inputs for the following visualization modules:

- → **T6.7** developing the VIA interface
- → **T7.2** creating the interface with visualisation libraries for immersive applications
- → **T7.3** developing geo-spatial data visualisation
- → **T7.4** developing graph network visualisations.

1.3 PURPOSE OF THE DELIVERABLE AND INTENDED AUDIENCE

The key objective of D6.1 is to identify and recommend investigative tools, methods and capabilities which could be undertaken by the subsequent AI-based tasks within INFINITY.

To this end, potential AI applications were extracted from the provided use case descriptions, while LEA partners and technical partners were asked to independently suggest AI applications which they would like to see being developed within the project. Based on those suggestions, AI applications were organised as modules in a number of AI toolboxes, which constitute the key contribution of D6.1: an organized set of AI-related tools that are recommended to be addressed in future development tasks. Finally, each toolbox was evaluated by technical partners in terms of its feasibility within the project (considering available know-how, time and resources and data availability among the partners). Based on this evaluation, this report provides a final list and ranking of recommended AI applications that are relevant to both LEAs and technical partners and at the same time seem to be viable within the scope of INFINITY. For lower ranked toolboxes that achieved low scores in more than one category, recommendations are provided on how to address the detected issues. As partner names are provided, the final evaluation also provides initial points of contacts, and an idea of which partner may be able to provide know-how and/or data required for a specific development.

The intended audience is thus predominantly constituted by technical partners and task leaders that are responsible for developing AI-based tools in future tasks, such as CERTH (T5.2, T6.3), KINEVIZ (T6.4), ENG (T6.5), DFKI (T6.6) and VICOM (T6.2).

1.4 DELIVERABLE STRUCTURE

This report is structured as follows. Chapter 2 provides a brief overview of the three use cases planned for INFINITY. A list of potential AI applications is extracted for each use case. Chapter 3 summarises the “wish list” of relevant AI applications as desired by LEA partners. Chapter 4 in turn presents AI methods and tools suggested by technical partners. Chapter 5 aims to combine results from Chapter 3 and 4 to generate a comprehensive overview of relevant AI applications, which are organised in modules as part of a total of seven AI toolboxes. Further, Chapter 5 includes a point-based evaluation of feasibility of each AI toolbox, filled out by each partner. Chapter 6 then analyses the results of this evaluation and finally provides a list of relevant and feasible AI applications, which shall serve as a recommendation to be taken into account in future AI-related development tasks within the project. Chapter 7 briefly summarises the outcomes of the previous chapters and provides some guidelines regarding potential next steps.

2 INFINITY USE CASE OVERVIEW AND POTENTIAL INVOLVEMENT OF AI

In order to apply and test the technologies and tools that are being developed within INFINITY in realistic scenarios, three use cases were developed. Use case 1 focusses on a cybercrime-related scenario, use case 2 on the aftermath of a terrorist attack and use case 3 is a hybrid scenario, combining cybercrime and counter terrorism. Since the AI applications to be recommended in this report should be aligned with requirements posed by the three use cases, the following section provides a brief overview of each use case scenario and a summary of the respective, potentially relevant AI applications.

2.1 USE CASE 1: ANALYSIS OF CYBER ATTACK BEHAVIOUR [ONGOING EVENT]

2.1.1 GENERAL DESCRIPTION

Use case 1 presents an ongoing cyber-attack scenario. A ransomware virus infiltrates a national public transport IT infrastructure, paralysing functionality and stealing sensitive information. To restore functionality of public transport websites and unlock compromised databases, the virus demands a payment in bitcoins.

2.1.2 AI APPLICATION POTENTIAL

Generally, AI-based tools could assist investigators in this cyber-attack scenario by clustering, classifying and prioritising the incoming information from various sources (news, internet, LEA databases, server logs, social media, bitcoin transactions, etc.) and filtering out concise, relevant information or additional knowledge. Specifically, AI may be useful for:

- Classification of constituent components of the attack
- Detection of suspicious data streams within the attacked infrastructure
- Detection and visualisation of attack routes and comparison of emerging patterns to previous cases (i.e., correlating the attack with similar known cyber-attacks)

It is to be noted that those are *suggested* AI applications only, based on a revision of this use case. It is not implied that all these aspects will need to be implemented within INFINITY.

2.2 Use Case 2: Rapid Analysis in the Aftermath of a Terrorist Attack [Post Event]

2.2.1 General description

Use case 2 presents a counter terrorism scenario, just after the attack has occurred (*post event*). An explosion with many victims takes place at a central train station in Member State A (MS-A); the attacker left behind an explosive device and has escaped; MS-A needs to locate and apprehend him whilst uncovering his network and finding potential accomplices/sympathizers who may commit further attacks. In the immediate aftermath of a terrorist attack, enormous amounts of structured and unstructured data from various sources (news, internet, CCTV footage, phone records, social media, LEA databases, traffic data, etc.) are collated.

2.2.2 AI application potential

Similar to use case 1, AI-based tools may be useful for classifying and organizing all incoming data, in order for investigators to be able to build a consistent and complete picture of the current situation. Specifically, AI may assist investigators via:

- Cross-referencing diverge data and visually highlighting the results in the 3D representation of the crime scene
- Suggesting most efficient and conclusive visualizations.

It is to be noted that those are *suggested* AI applications only, based on a revision of this use case. It is not implied that all these aspects will need to be implemented within INFINITY.

2.3 Use Case 3: Hybrid Threats – The convergence of cyber and terrorism [Preventative]

2.3.1 General description

Use case 3 presents a hybrid cyber-attack and terrorism scenario in which terrorists try to attack critical infrastructure sites in coordination with physical attacks whilst sites are weakened by cyber-attacks. This is a *preventative* scenario, in which INFINITY tools shall help uncovering the imminent attack before it happens. An anarchist extremist group has been growing in popularity across member state MS-A and the group has repeatedly called for the abolishment of national borders and for dedicated cyber takedowns of border, LEA and governmental online infrastructure.

A critical question to be addressed when trying to prevent the imminent attack is, for example, to continuously update the existing case profiles with new points of interest (POIs) and concerns in order to alert case investigators timely.

2.3.2 AI application potential

As in the previous use cases, AI-based tools can help to categorise, cluster, classify and organise incoming data; in this use case it is especially important to have automated, continuous scraping, screening and classification services dealing with incoming information and generating alerts prior to the attack. Specifically, AI could assist investigators by:

- Filtering and matching relevant open-source data that are fed into INFINITY
- Comparing detected patterns to historical data from previous incidents to generate alarms.

It is to be noted that those are *suggested* AI applications only, based on a revision of this use case. It is not implied that all these aspects will need to be implemented within INFINITY.

3 POTENTIAL AI APPLICATIONS FOR INFINITY PROPOSED BY LEAS

Based on the previously described use cases, LEA and LEA-related partners were asked to propose AI applications which they deem to be useful and relevant for INFINITY. The idea was to generate an exhaustive "wish list" of AI applications, which could then eventually be matched with a list of possible solutions that are *independently* proposed by technical partners (see chapter 4). The following sections detail all desired applications proposed by LEA partners, without taking into account technical feasibility or any other criteria.

3.1 GENERAL TEXT PROCESSING

3.1.1 SPEECH TO TEXT

Relevant for use cases: UC1, UC2, UC3

Description: Convert audio files or videos containing audio into text.

Functionality: Using an audio file, a video or a set of multiple audio files and videos containing audios, the tool would convert the audio of each video into a text.

3.1.2 AUTOMATIC MULTILANGUAGE TRANSLATION OF TEXTS

Relevant for use cases: UC1, UC2, UC3

Description: Text is automatically translated from the original language to another language selected by the user.

Functionality: The tool would have a text or a set of multiple texts as an input and would automatically translate them from the original language into a language selected by the user. The tool would be able to recognise the origin language of the input text.

3.1.3 ENTITY EXTRACTION FROM TEXT

Relevant for use cases: UC1, UC2, UC3

Description: Text is analysed and relevant entities (location, date and time, etc.) are extracted from the text.

Functionality: A text or a set of multiple texts would be used as an input. The tool would identify the different entities contained in the texts (location, organisations, date…) and would extract them. This tool could also work in an analytical tool and create a link chart between the original text and the extracted entities.

3.1.4 SENTIMENT ANALYSIS OF TEXT

Relevant for use cases: UC1, UC2, UC3

Description: Text is analysed, and the sentiment of the message is identified (e.g., hate speech, violent, threatened, peaceful, aggressive…)

Functionality: A text or a set of multiple texts would be used as an input. The tool would analyse the content of each text and would tell the user the sentiment of the author of each text (anger, fear, happiness, optimistic…).

3.1.5 SUMMARISATION

Relevant for use cases: UC1, UC2, UC3

Description: Analysis and summarisation of a long text into a short text. Include the possibility to represent the text under a word cloud.

Functionality: A text or a set of multiple texts would be used as an input. The tool would analyse the content of each text and summarise each of them.

3.2 IMAGE AND VIDEO PROCESSING

3.2.1 IMAGE RESOLUTION ENHANCER

Relevant for use cases: UC1, UC2, UC3

Description: Enhance the quality of the resolution of a picture or a video.

Functionality: Based on single or multiple pictures or videos, the tool would enhance the quality of the media by producing the same images/videos at a higher resolution.

3.2.2 VIDEO STABILISATION

Relevant for use cases: UC1, UC2, UC3

Description: Remove abrupt and irregular camera motions and transform the input sequence to a stable and visually plausible video.

Functionality: Based on a video or a set of multiple videos, the tool would create a more stable version of the same videos.

3.2.3 3D CRIME SCENE BUILDER

Relevant for use cases: UC2

Description: Build a 3D/4D (3D + time) crime scene based on different photos and videos of the same location.

Functionality: The tool would reconstruct a 3D crime scene using videos and photos taken of the place at different times. It would be possible to display the crime scene at different moments based on the input videos and photos.

3.3 IMAGE AND VIDEO CLASSIFICATION

3.3.1 DEEP FAKE DETECTION

Relevant for use cases: UC1, UC2, UC3

Description: Analysis of a video to detect if the content is real or created using deep fake technologies.

Functionality: The tool would analyse a video or a set of videos and check if there were any use of deep fake technologies to create the media.

3.3.2 PROPAGANDA VIDEO IDENTIFICATION

Relevant for uses cases: UC2, UC3

Description: Analyse a video and identify if it contains terrorist propaganda content.

Functionality: Scan frames and audio of a video and analyse if there is any content linked to terrorist propaganda.

3.4 IMAGE- AND VIDEO ANALYSIS: OBJECT, TEXT DETECTION AND RECOGNITION

3.4.1 OBJECT DETECTION, CLASSIFICATION AND TRACKING

Relevant for use cases: UC1, UC2, UC3

Description: Detect and classify extracted objects from a picture or a video according to defined categories (e.g., car, weapon, object, …).

Specific applications: Identify and track vehicles featured in videos; automatically count how many people are featured in an image or video.

Functionality: Videos and pictures would be used as an input. The tool would analyse them to detect, identify, tag and annotate (bounding boxes) all the objects featured on the media.

3.4.2 TEXT DETECTION AND EXTRACTION IN IMAGE AND VIDEO DATA

Relevant for use cases: UC1, UC2, UC3

Description: Identify when text is written / edited on pictures and in videos and extract the text.

Functionality: Videos and pictures would be used as an input. The tool would analyse them to detect and extract any written text readable on the media. The tool should be able to extract text from elements of the pictures and the videos but also the text edited on them.

3.5 SOCIAL MEDIA ANALYSIS

3.5.1 IDENTIFICATION OF FAKE SOCIAL MEDIA ACCOUNTS

Relevant for use cases: UC1, UC2, UC3

Description: Analysis of social media accounts to identify those who are managed by a bot or anonymisation software.

Functionality: Based on different criteria, the tool would identify if social media accounts are managed by a bot.

3.5.2 EVENT DETECTION

Relevant use cases: UC1, UC2, UC3

Description: Text scraped from social media (including forums, blogs etc.) is analysed and the tool can identify specific events such as support for criminal groups, intention to commit a crime, glorifying crimes, expressing

intention to join a criminal group, encouraging support of a criminal group or planned target locations and time of attack.

Functionality: A text mined from the web (e.g., texts retrieved from social media via advanced keyword-based search), or a set of multiple texts would be used as an input. The tool would analyse the content of each text and would tell the user if a specific event is mentioned. Alarms for potential future threats or planned attacks could be triggered and shown to the investigators.

3.6 MALWARE AND CYBER-ATTACK ANALYSIS

3.6.1 MALWARE AND ATTACK ANALYSIS

Relevant for use cases: UC1, UC3

Description: Analyse information gathered from static, black-boxing and white-boxing analyses to identify patterns and trends in malware structures, behaviours and payloads. Classification of constituent components of the attack.

Functionality: Based on identified trends and patterns, the tool would analyse information extracted from malwares to identify possible relevant information for the investigation. Suspicious data streams within the attacked infrastructure could be detected.

3.6.2 AI PATTERN RECOGNITION

Relevant for use cases: UC1, UC2, UC3

Description: Analysis of large datasets and identify all possible common trends and patterns, for example to uncover illicit or abnormal behaviour in transactions, server logs or user behaviour within cryptocurrency networks or fiscal data.

Functionality: Based on previous cases, the tool would learn how to identify patterns and trends relevant for the investigation. Attack patterns could be visualised and compared to similar known previous cyber-attacks.

3.6.3 BITCOIN BLOCKCHAIN ANALYSIS

Relevant for use cases: UC1, UC3

Description: Advanced analysis of transactions in blockchains related to crypto-currencies and identification of patterns and bitcoin entities.

Functionality: Based on known patterns and trends in relation to crypto-currency transactions, the tool would analyse the blockchains starting from specific selectors linked to the suspects. Specific services and dark markets can be monitored for relevant new entries.

3.7 OTHER DATA ANALYSIS

3.7.1 GEOLOCATION DATA ANALYSIS AND VISUALISATION

Relevant for use cases: UC1, UC2, UC3

Description: Connect any kind of incoming, case-relevant data to geolocation data.

Functionality: Generally, the tool aims to connect all incoming information (from various data sources such as image, video, voice, news, social media, bitcoin, phone record data, etc.) to geolocation data to map potential origin and destination locations. Relevant geo-based events could be plotted on an interactive map.

4 POTENTIAL AI APPLICATIONS FOR INFINITY PROPOSED BY TECHNICAL PARTNERS

Technical partners were in turn asked to independently propose a list of potential AI applications that they deem to be relevant and technically feasible within INFINITY. The following sections detail those proposals. However, the applications listed here may not represent what will be implemented within the scope of INFINITY. It is to be noted that the "wish list" of AI applications desired by LEAs as presented in chapter 3 was not accessible for technical partners.

4.1 IMAGE- OR VIDEO-BASED AI

4.1.1 OBJECT DETECTION FROM VIDEO DATA

Relevant for use cases: UC1, UC2, UC3

Description: Automatically identify specific objects in any video footage that can be of any relevance for an investigation.

Functionality: Object recognition systems can recognize, identify and locate objects within a video with a given degree of confidence.

Use: Object recognition from CCTV data is useful for detecting elements that may provide additional information for investigators and may be able to identify explosives or suspicious objects.

4.1.2 OBJECT DETECTION IN HARSH ENVIRONMENTS

Relevant for use cases: UC2, UC3

Description: Detection of objects in images and videos taking into account the special case where environmental conditions are difficult (low-light, rain, low resolution, etc.); "object detection in the wild".

Functionality: Images and videos recorded by CCTV cameras or mobile phones often show low image quality, making it difficult to discern details of objects. This tool could help improve image resolution or stabilise videos via image processing algorithms prior to object detection.

Use: Detecting suspicious objects in low-quality images and videos recorded in harsh environments is crucial for screening social media content and for detecting, tracking and identifying objects in use case 2 and use case 3, for example.

4.1.3 VIDEO SUMMARISATION

Relevant for use cases: UC2, UC3

Description: Automatic generation of a short summary of the content of a longer video document by selecting and presenting the most informative or interesting materials for potential users (LEAs).

Functionality: The aim of video summarization is to speed up browsing of a large collection of videos and achieve efficient access and representation of the video content. By watching the summary, users can make quick decisions on the usefulness of the video. Dependent on applications and target users, the evaluation of summary often involves usability studies to measure the content informativeness and quality of a summary.

Use: This technology can be useful for extracting useful information from social media platforms or CCTV footage.

4.2 TEXT-BASED AI (NLP)

4.2.1 SOCIAL NETWORK ANALYSIS

Relevant for use cases: UC1, UC2

Description: To provide accurate early warnings of security crises, detailed post-incident factual information as well as overall intelligence analysis.

Functionality: Social Network Analysis (SNA) is able to provide efficient exploitation of massive data streams with the end goal of capturing the overall organization of criminal networks orchestrating attacks and the interrelations of its members, identifying key individuals and providing timely risk and threat assessment.

Use: This proposed AI application is aligned with the first two of the INIFINITY use cases. More specifically, in the first use case SNA can assist in identifying similar cyberattacks occurring in other public services while in the second use case information about the (occurred) attack can be enhanced through live content shared by on-site bystanders.

4.3 OTHER AI APPLICATIONS

4.3.1 EVENT AND TREND DETECTION

Relevant for use cases: UC1, UC2

Description: This AI application aims to identify trending topics in networks of specific events which are of interest in the investigative processes.

Functionality: At first, this application determines whether the data collected among heterogeneous sources are related to a specific event of interest. Then, the event-related data are analysed in order to discover unidentified trending topics within networks.

Use: It is mainly aligned with the first two use cases, where the event and trend detection module would assist in the identification of data which are related to the cyber-attack event (UC1) or to the terrorist attack event (UC2) along with the detection of trending topics in them.

5 PROPOSED AI TOOLBOXES FOR LAW ENFORCEMENT AGENCIES WITHIN INFINITY

Based on the two lists of possible AI applications - proposed by LEAs and by technical partners without knowing the content of the respective other list - in this chapter, relevant AI toolboxes which could be developed within INFINITY are suggested. Each toolbox addresses common points taken from both lists and tries to organise the previously presented content within suitable technological themes. It is to be noted that all proposed toolboxes will need to be assessed against end-user requirements to be defined in D3.4. Toolboxes were derived merely based on the information provided within this report and by no means are definite or binding.

After compiling the list of toolboxes, partners were asked to evaluate each toolbox in terms of their respective technical *know-how*, *data availability* and overall *feasibility* within INFINITY. Note that such detailed evaluation was only asked to be filled out by *technical* partners. Non-technical partners such as LEAs were only asked to fill out the data availability column (marked as "OTHER PARTNERS" in the respective tables). Evaluation scores (ranging from 0 = low to 3 = high) are shown in this chapter in an additional table at the bottom of each toolbox. Highest scores for each category are marked in bold. Only the maximum score was considered as one partner assigning a high score (2-3) was assumed to be sufficient to cover a category well. The final overall score for each toolbox was calculated as the average of the three maximum scores obtained for each category. A detailed explanation of the evaluation methodology and results of this evaluation are presented in chapter 6.

Partners could also add their interest for developing specific toolbox modules. This indication however is not binding and only serves as a guideline of which partner may be contacted in case it is decided that a specific module shall be developed. Fields marked with a "-" sign indicate no answer from any partner at the time of submitting the report. In case a specific toolbox results to be of interest in the future, those fields indicate open questions related to the toolbox that may need to be addressed.

5.1 TEXT PROCESSING AI TOOLBOX

TEXT PROCESSING AI TOOLBOX		
Purpose (end-user focused)	Assist investigators in quickly extracting key information from a large number of text documents obtained from various sources	
Short description	The text processing toolbox would help converting recorded audio into written text, potentially translate texts from/to various languages, quickly extract key information regarding locations, times and dates etc., would be able to extract text sentiment (positive, negative, threatening, aggressive key messages) and would help summarising large text documents in short abstracts.	
Alignment with INFINITY Use Cases	UC1, UC2, UC3	
Aligned with developments in task(s):	T6.3, T6.5	
Potential modules	**Module name**	**Interested technical partners**

	Speech-to-text	-
	Automatic Multilanguage Translator	-
	Entity extractor	**CERTH, DFKI**
	Sentiment analyser	**CERTH, DFKI**
	Text summariser	**DFKI**
Potential data sources	Example data available.	
Potential database types	-	
Potential Machine Learning / AI methods	-	
Potential known benchmarks	-	
Potential output formats and visualizations	-	

Evaluation (0-3 points)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	**2**	**2**	1	**2**	1	**2**	**2**	-	***2***
Feasibility given time and resources	0	**2**	0	**2**	0	0	0	-	***2***
Data availability	1	1	0	0	0	0	0	***2***	***2***
Overall Score	***2***								

5.2 OTHER DATA ANALYSIS TOOLBOX

OTHER DATA ANALYSIS TOOLBOX		
Purpose (end-user focused)	Assist investigators in quickly analysing case-relevant data from other, specific data sources such geolocation data	
Short description	During an investigation, apart from the aforementioned data sources, other data sources may become available, such as geolocation data. This module could connect incoming data from various sources (web scraping, etc.) to geolocation data and map potential locations of objects or events.	
Alignment with INFINITY Use Cases	UC1, UC2, UC3	
Aligned with developments in task(s):	T6.3, T6.4, T6.5	
Potential modules	**Module name**	**Interested technical partners**
	Geolocation extractor	**VICOM**
Potential data sources	Example data available.	
Potential database types	-	
Potential Machine Learning / AI methods	-	
Potential known benchmarks	-	
Potential output formats and visualizations	-	

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	2	0	1	**3**	0	2	0	-	**3**
Feasibility given time and resources	1	0	1	**3**	0	2	0	-	**3**
Data availability	1	0	**2**	1	0	0	0	1	**2**
Overall Score	**2.7**								

5.3 MALWARE AND CYBER-ATTACK TOOLBOX

MALWARE AND CYBER-ATTACK TOOLBOX		
Purpose (end-user focused)	Assist investigators in identifying malware, suspicious data streams, attack patterns and constituent components as well as patterns related to crypto-currency transactions	
Short description	The malware and cyber-attack toolbox could assist in identifying anomalies, trends and patterns in server logs, data streams or crypto-currency networks that could lead to classifying constituent components of an attack or to identifying potentially relevant locations or suspects.	
Alignment with INFINITY Use Cases	UC1, UC3	
Aligned with developments in task(s):	T6.3, T6.4, T6.5	
Potential modules	**Module name**	**Interested technical partners**
	Malware and server log analyser	-
	Crypto-currency analyser	-
Potential data sources	Malware sample, server logs and crypto-currency transactions would be needed. Anonymised data could be provided for malware sample and server logs.	
Potential database types	-	
Potential Machine Learning / AI methods	-	
Potential known benchmarks	-	
Potential output formats and visualizations	-	

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	0	0	**1**	**1**	0	**1**	0	-	***1***
Feasibility given time	0	0	**2**	1	0	0	0	-	***2***

and resources									
Data availability	0	0	1	1	0	0	0	***1.5***	***1.5***
Overall Score	***1.5***								

5.4 SOCIAL MEDIA TOOLBOX

SOCIAL MEDIA TOOLBOX		
Purpose (end-user focused)	Assist investigators in detecting fake social media accounts, extracting relevant social media networks and automatically extracting case-relevant information (pre, ongoing and post event) from multiple social media sources	
Short description	The social media toolbox could help find fake social media accounts that are managed by bots or have been altered by anonymisation software, for example.	
Alignment with INFINITY Use Cases	UC1, UC2, UC3	
Aligned with developments in task(s):	T6.3, T6.4, T6.5	
Potential modules	**Module name**	**Interested technical partners**
	Fake account identifier	**-**
	Social network analyser	**CERTH, VICOM**
	Event and trend extractor	**CERTH**
Potential data sources	Example data available.	
Potential database types	-	
Potential Machine Learning / AI methods	Various AI techniques such as: ● Natural Language Processing ● Named Entity Recognition ● Entity Linking	

	• Sentiment Analysis Clustering, classification and outlier detection algorithms: • (Madani et al., 2015) • (Panagiotou et al., 2016) • (Michaelis, S., Piatkowski, N., & Stolpe, 2016) Deep learning: • (Feng et al., 2018) • (Nguyen et al., 2019) • (Bouindour et al., 2019)
Potential known benchmarks	Networks extracted through online APIs (e.g., NodeXL) could service as potential benchmarks. The dataset mentioned (McMinn et al., 2013) can be used as a benchmark.
Potential output formats and visualizations	The results of the algorithms could be in simple format including information about: • The starting time of an event • The ending time of the event • The identity of a detected trend(s) related to the event • The name of the detected trend(s) • The confidence score for the identification of the trend(s)

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	**3**	0	1	2	0	2	2	-	***3***
Feasibility given time and resources	**2**	0	**2**	**2**	0	1	0	-	***2***
Data availability	1	0	**2**	1	0	0	0	***2***	***2***
Overall Score	***2.3***								

5.5 IMAGE AND VIDEO PROCESSING TOOLBOX

IMAGE AND VIDEO PROCESSING TOOLBOX	
Purpose (end-user focused)	Assist investigators when analysing a large number of (low-quality) images and videos by enhancing, stabilising, reconstructing or

	summarising their content	
Short description	As investigators often have to deal with low-quality (low-resolution, unstable, low light) image and video data recorded with a multitude of different recording devices, the image and video processing toolbox could assist in automatically improving image and video quality as well as in reconstructing a crime scene in 3D (or in 4D, including a time dimension) using input from various cameras. Furthermore, long video content could be summarised by automatically selecting and presenting the most informative or interesting material.	
Alignment with INFINITY Use Cases	UC2, UC3	
Aligned with developments in task(s):	T5.2	
Potential modules	**Module name**	**Interested technical partners**
	Image resolution enhancer	**CERTH, VICOM**
	Video stabiliser	-
	Video summariser	**DFKI**
Potential data sources	Example data available.	
Potential database types	-	
Potential Machine Learning / AI methods	Video summarization is mainly addressed by different variants of Deep Learning: ● Deep reinforcement learning ● Self-attention mechanisms combined with bi-directional recurrent networks (BiLSTM)	
Potential known benchmarks	Summary benchmarks are available on the following site: https://paperswithcode.com/task/video-summarization	
Potential output formats and visualizations	The output of the video summarization tool is a condensed (shorter) video showing the main elements and actions of the long video, that can be easily used by the end users in a short amount of time.	

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max.**

									Score
Technical know-how	2	**3**	0	1	1	2	0	-	***3***
Feasibility given time and resources	0	**3**	1	2	0	1	0	-	***3***
Data availability	1	0	1	1	0	0	0	***3***	***3***
Overall Score	***3***								

5.6 IMAGE AND VIDEO CLASSIFICATION TOOLBOX

IMAGE AND VIDEO CLASSIFICATION TOOLBOX		
Purpose (end-user focused)	Assist investigators in detecting fake and propaganda videos as well as in identifying the locations where images and video may have been taken	
Short description	The image and video classification toolbox could analyse videos found on social media, for example, and classify them as being fake or real (deep fake detection).	
Alignment with INFINITY Use Cases	UC2, UC3	
Aligned with developments in task(s):	T5.2, T6.3	
Potential modules	**Module name**	**Interested technical partners**
	Deep fake detector	-
	Propaganda video identifier	**CERTH**
Potential data sources	Example data available.	
Potential database types	-	
Potential Machine Learning / AI methods	-	

Potential known benchmarks	-
Potential output formats and visualizations	-

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	**1**	**1**	0	**1**	**1**	**1**	0	-	**1**
Feasibility given time and resources	0	0	**1**	**1**	0	0	0	-	**1**
Data availability	1	0	1	0	0	0	0	***3***	**3**
Overall Score	**1.7**								

5.7 OBJECT DETECTION TOOLBOX

OBJECT DETECTION TOOLBOX		
Purpose (end-user focused)	Assist investigators in automatically detecting, tagging, tracking and identifying various types of case-relevant objects (weapons, explosives, cars, etc.) in image or video data	
Short description	Object recognition systems can recognize, identify and locate objects within an image or video with a given degree of confidence.	
Alignment with INFINITY Use Cases	UC2, UC3	
Aligned with developments in task(s):	T5.2	
Potential modules	**Module name**	**Interested technical partners**
	General object detector	**UPM, CERTH**
	Object detector for harsh environments	**DFKI, CERTH**

	Text and number plate extractor	**CERTH, DFKI, UPM**
Potential data sources	Example data available.	
Potential database types	COCO dataset – This is one of the most known datasets for object detection and is usually the one used for testbench the algorithms performance. It is composed by 80 classes with several types of objects (animals, furniture, clothing…). (Lin et al., 2014) https://cocodataset.org/#home"https://cocodataset.org/#home OpenImages - Open Images dataset is composed by a wide range of images annotated with image-level labels, object bounding boxes, object segmentation masks, visual relationships, and localized narratives. It contains a total of 16M bounding boxes for 600 object classes on 1.9M images, making it the largest existing dataset with object location annotations. The boxes have been largely manually drawn by professional annotators to ensure accuracy and consistency. The images are very diverse and often contain complex scenes with several objects (8.3 per image on average). (Kuznetsova et al., 2018) https://storage.googleapis.com/openimages/web/index.html Berkeley Deep Drive - BDD100K is the largest driving video dataset with 100K videos and 10 tasks to evaluate the exciting progress of image recognition algorithms on autonomous driving. The dataset possesses geographic, environmental, and weather diversity, which is useful for training models that are less likely to be surprised by new conditions. It provides 2D Bounding Boxes annotated on 100,000 images for bus, traffic light, traffic sign, bike, truck, motor, car, train, and rider. (Yu et al., 2018) https://bdd-data.berkeley.edu/ Objects365 - Large-scale object detection dataset which has 365 object categories over 600K training images. More than 10 million, high-quality bounding boxes are manually labelled through a three-step, carefully designed annotation pipeline. (Shao et al., 2019) http://www.objects365.org/overview.html Specific purpose datasets – There are millions of datasets, depending on the application under development. There are datasets for animals, traffic signs, tumours, text etc. Further research is needed to find the best suitable dataset for the project or even create a new one manually.	

Potential Machine Learning / AI methods	Mainly deep learning algorithms. The balance between accuracy and detection time depends on the task to be performed. Some algorithms sacrifice accuracy in order to get high processing throughput (real-time). On the other side, some algorithms provide very accurate results but are far from real-time processing capabilities. The three most known families of algorithms are RCNN, YOLO and SSD. The most used versions of each of them can be found in: • (He et al., 2020) • (Bochkovskiy et al., 2020) • (Shi et al., 2019) The first one provides a very accurate but slow and difficult to run in real-time solution. Nevertheless, this algorithm is also able to work with segmentation masks. The second is the last version of YOLO algorithms family and provides a good balance between accuracy and speed achieving real time processing. The last versions of SSD algorithms are achieving good accuracy and the performance is slightly better for real-time. Finally, the accuracy-based top algorithms in the COCO test-dev dataset are: • (C. Y. Wang et al., 2020) • (Tan et al., 2019)
Potential known benchmarks	There are several benchmarks depending on the task to be performed. The most used for performance evaluation is the COCO test-dev dataset. The accuracy of the top algorithms can be extracted from the following links using different benchmark datasets: COCO test-dev: https://paperswithcode.com/sota/object-detection-on-coco PASCAL VOC 2007: https://paperswithcode.com/sota/object-detection-on-pascal-voc-2007 KITTI: https://paperswithcode.com/sota/object-detection-on-kitti-cars-easy CrowdHuman: https://paperswithcode.com/sota/object-detection-on-crowdhuman-full-body Depending on the complexity of the backbone used, these two algorithms can achieve real time capabilities.
Potential output formats and visualizations	The algorithms provide simple output formats that usually contain the following data for each detected object: • Bounding box – xs, ys, xi, yi. Coordinates of the top corner and bottom opposite corner of the bounding box. • Class – Identifier of the detected class. • Probability – Value between 0-1 range providing the detection

	accuracy. Some algorithms can perform both object detection and segmentation at the same time when segmentation masks are available. In this case, the coordinates of the segmentation masks are also provided (segmentation mask – list [x1, y1, x2, y2, … xn, yn]. Point to get the detected shape of the object). The visualization is a postprocess where the detected data is drawn over the images. Bounding boxes can be included together with the name of the class and the probability. Segmentation masks can be also drawn over the detected object.

Evaluation (0-3)									
Criterion	**CERTH**	**DFKI**	**KEMEA**	**KINEVIZ**	**UPM**	**VICOM**	**ENG**	**OTHER PARTNERS**	**Max. Score**
Technical know-how	**3**	**3**	1	0	**3**	1	0	-	***3***
Feasibility given time and resources	2	**3**	2	0	**3**	1	0	-	***3***
Data availability	2	1	**3**	0	**3**	0	0	***3***	***3***
Overall Score	***3***								

6 EVALUATION AND RECOMMENDATION OF PROPOSED AI TOOLBOXES FOR INFINITY

The seven AI toolboxes proposed in the previous chapter were each evaluated by all partners with respect to three categories:

- **Know-how** of the respective partner to participate in development tasks related to this toolbox
- Estimated **feasibility** to develop AI-based applications related to the toolbox given the remaining time and resources available within INFINITY
- Training **data availability**

For each category, scores between 0 (low) and 3 (high) could be given. Toolboxes that score low in all three categories are hence considered to be relevant and interesting from the LEAs' perspective yet may not be possible to be developed entirely within the scope of INFINITY. Furthermore, the separation into three categories allows detecting issues that could potentially be resolved prior to starting development. Low scoring for know-how and data availability may be improved by exchanging knowledge and data among partners or could motivate building up missing know-how or gathering new data from scratch. Low feasibility scores generally are difficult to overcome as partners in this case considered time and available resources provided within INFINITY to be insufficient. The evaluation presented in this chapter is meant to provide a guideline for task leaders organising further development within AI-related tasks in WP5 and WP6. It is to be noted that independently of the presented evaluation results, all toolboxes will need to be evaluated with respect to end-user- requirements to be defined in D3.4.

6.1 EVALUATION METHODS

The actual scores are detailed in chapter 5 in a table placed at the bottom of each AI toolbox. Highest scores for each category were marked in bold. Only the maximum score was considered as one partner assigning a high score -was assumed to be sufficient to cover a category well. The final overall score for each toolbox was calculated as the average of the three maximum scores obtained for each category. According to the scores, toolboxes were classified into "highly feasible", "feasible" and "not ready for development". The latter class indicates toolboxes that are relevant, yet partners gave low scores in more than one category. For those toolboxes, recommendations how to address such low scores are provided. All scores provided by the involved partners were estimated and are non-binding in the sense that high know-how or feasibility scores, for example, do not imply binding commitment to carry out development within a toolbox.

6.2 EVALUATION RESULTS

An overview of the final ranking in terms of feasibility is provided in Table 1. Two toolboxes achieved the best possible overall score of 3 (toolbox *5.5 Image and Video Processing*, *5.7 Object Detection*); toolboxes 5.2 (*Other Data*) and 5.4 (*Social Media*) scored just under 3 and 5.1 (*Text Processing*) scored a good overall value of 2. The two lowest scoring toolboxes were 5.6 (*Image and Video Classification*) and 5.3 (*Malware and Cyber-attacks*). Detailed evaluations are given in the following sections.

Table 1: Toolbox feasibility ranking

No.	Toolbox name	Score range	Classification	Ranking
5.5	**Image and video processing toolbox**	Best scoring	Highly feasible	**1**
5.7	**Object detection toolbox**	Best scoring	Highly feasible	**2**
5.2	**Other data analysis toolbox**	High scoring	Feasible	**3**
5.4	**Social media toolbox**	High scoring	Feasible	**4**
5.1	**Text processing AI toolbox**	Mid-range	Feasible	**5**
5.6	**Image and video classification toolbox**	Low scoring	Not ready for development	**6**
5.3	**Malware and cyber-attack toolbox**	Low scoring	Not ready for development	**7**

6.2.1 BEST SCORING TOOLBOXES (HIGHLY FEASIBLE)

The best scoring toolboxes were toolbox *5.5 Image and Video Processing* and *5.7 Object Detection,* which scored full 3 points regarding know-how, feasibility and data availability and thus overall scored the best possible score of 3. Based on these results, core development within INFINITY will likely focus on AI--based tools associated with these toolboxes.

For toolbox 5.5 *(Image and Video Processing)*, DFKI, CERTH and VICOM could provide technical know-how; DFKI and KINEVIZ considered development feasible and CERTH, KEMEA and KINEVIZ could provide data.

For 5.7 *(Object Detection)*, especially CERTH, DFKI and UPM could provide know-how and all these partners considered development feasible. In addition, KEMEA and UPM could provide training data.

6.2.2 HIGH SCORING TOOLBOXES (FEASIBLE)

The two toolboxes achieving high scores just below 3 were *5.2 Other Data* with an overall score of 2.7 and *5.4 Social Media* with a score of 2.3. For both toolboxes, very good know-how is available among the partners (both scoring 3 in this category), while data availability is slightly lower, yet in a good range.

For toolbox 5.2 *(Other Data)*, KINEVIZ, CERTH and VICOM could provide know-how and both KINEVIZ and VICOM considered development to be feasible. In terms of data availability, only KEMEA scored a 2, while CERTH and KINEVIZ scored a 1. It would need to be revised which kind of data is available that allows developing AI--based tools.

For toolbox 5.4 *(Social Media)*, CERTH, KINEVIZ, VICOM and ENG could provide technical know-how and CERTH, KEMEA and KINEVIZ deemed this task to be feasible. In terms of data availability, KEMEA scored a 2.

6.2.3 MID-RANGE SCORING TOOLBOXES (FEASIBLE)

Toolbox *5.1 Text Processing* achieved a score of 2 overall and across all categories and thus show good potential to be realised within INFINITY.

For 5.1 *(Text Processing)*, CERTH, DFKI, KINEVIZ, VICOM and ENG could provide know-how, while DFKI and KINEVIZ considered development to be generally feasible. CERTH and DFKI could provide input data.

6.2.4 LOW SCORING TOOLBOXES (NOT READY FOR DEVELOPMENT)

The three critical toolboxes that were overall scoring low (below 2) were toolbox *5.6 Image Classification* and toolbox *5.3 Malware and Cyber-attacks*.

Toolbox 5.6 *(Image Classification)* obtained low feasibility scores and additional low know-how scores of 1. The recommendation of this report is to revise among technical partners whether the required know-how could potentially be built-up allowing for smaller development tasks in the area of image or video classification.

Finally, toolbox 5.3 *(Malware and Cyber-attacks)* obtained the lowest overall score of 1.5, mainly due to low know-how and low data availability. Yet, KEMEA considered development to be feasible. As cyber and malware attacks are mentioned in two INFINITY use cases, the recommendation of this report is to examine whether technical know-how could be built up among partners in order to enable development of at least one relevant module within this toolbox. Data availability seems to be an issue, however it is to be considered that, for example, crypto-currency-related data is publicly available under the online resources mentioned in chapter 5.5.

7 CONCLUSIONS

This report aims to provide a guideline for task leaders responsible of developing AI and ML-based tools and applications within INFINITY work packages (predominantly WP5 and WP6). Those tools need to be integrated into the planned immersive and interactive investigation platform in order to allow for efficient extraction and analysis of case relevant- data from various data sources. There are various tasks within INFINITY dedicated to developing AI-based tools:

- Object detection and recognition (T5.2)
- Activity detection and recognition (T5.2)
- Event and trend detection (T6.3)
- Social network analysis (T6.4)
- Graph analysis and recommendation engine (T6.4)
- Pattern recognition (T6.5)
- Virtual Investigative Assistant, recommender system (T6.6)

However, concrete applications and tools that involve AI and ML are yet to be defined. This report therefore first gathered an overview of potential AI applications based on the planned use cases. Based on this description, LEAs and technical partners were asked to independently propose desired or planned AI tools and applications they would like to see being developed within INFINITY. The first two results provided by this report are thus **a) a detailed list of relevant AI applications desired by LEAs**, presented in chapter 3 as well as **b) a list of AI tools suggested by technical partners**, presented in chapter 4.

Further, the two lists were joined by organising the proposed tools and applications in subtopics, trying to take into consideration all suggestions from both lists. The result of this operation is presented in chapter 5 and is given as a list of **seven AI toolboxes**, each one addressing a specific field of AI-based analyses, using different kinds of input data. For each toolbox, potential modules, as well as relevance for use cases, general purpose and functionality, potential data sources, techniques and benchmarks are provided wherever possible. The seven AI toolboxes are the following:

5.1 Text processing AI toolbox

5.2 Other data analysis toolbox

5.3 Malware and cyber-attack toolbox

5.4 Social media toolbox

5.5 Image and video processing toolbox

5.6 Image and video classification toolbox

5.7 Object detection toolbox

They constitute **a first recommendation of AI-based tools and applications which may be addressed by further development** within INFINITY. It is to be noted that all proposed toolboxes and their content are non-binding in the sense that task leaders and partners are not obliged to align all AI-related development with toolbox content. Toolboxes were meant to organise AI-based applications with respect to their relevance for LEAs and within technological categories that may serve as a guideline for further development within INFINITY. All toolboxes will need to be evaluated with respect to end-user requirements to be defined in D3.4 as well.

In a final step, all partners were asked to independently evaluate and score each toolbox in terms of available know-how, training data and feasibility. According to those scores, toolboxes were ranked as "highly feasible", "feasible" and "not ready for development".

The two "**highly feasible" toolboxes** with the highest scoring were toolbox ***5.5 Image and Video Processing*** *and* ***5.7 Object Detection***. According to the presented results, those toolboxes are highly relevant for LEA workflows, there is high knowledge and data availability among the partners and several partners deem development to be highly feasible.

The "**feasible" toolboxes**, which achieved slightly lower ranking, were (in order of ranking from higher to lower overall scores) toolbox ***5.2 Other Data*** and toolbox ***5.4 Social Media***, as well as toolbox ***5.1 Text Processing***. All of those are relevant, partners evaluated them as feasible and there is sufficient know-how and data available. For specific toolboxes, partners may need to determine which partner could provide technical knowledge to other partners and how data can be shared efficiently such that good training data is accessible for all involved partners (to this end, also outcomes from data related tasks such as D3.2 should be considered).

Finally, two toolboxes achieved low scores across the three categories and were thus classified as "**not ready for development"**. Those toolboxes were ***5.6 Image Classification*** and toolbox ***5.3 Malware and Cyber-attacks***. Toolbox *5.6 Image Classification* achieved low feasibility scores, and additionally had low know-how scores. Data availability however was scored high. Hence, the recommendation of this report is **to revise among technical partners whether the required know-how could potentially be built-up allowing for smaller development tasks in the area of image or video classification**. Lastly, toolbox *5.3 Malware and Cyber-attacks* obtained the lowest overall score, mainly due to low know-how and low data availability. However, one partner considered development to be feasible. As cyber and malware attacks are related to two INFINITY use cases, the recommendation of this report is **to examine whether technical know-how could be built up among partners and whether publicly available data could be exploited in order to enable development of an AI-based tool applicable to malware and cyber-attacks.**

It is to be noted that – in addition to the aforementioned recommendations – concrete **partners are named** for each toolbox and for each category. This shall provide **initial points of contact and a starting point for a discussion among interested partners concerning future AI-oriented development tasks** and generally aims to clarify individual partner objectives and capabilities. Overall, this report hopes to provide a guide and starting point for subsequent development tasks within WP5 and WP6, with the general aim of guiding towards the development of relevant and functional AI-based tools that can assist analysts and investigators by significantly enhancing investigative capabilities.

8 REFERENCES

Bochkovskiy, A., Wang, C.-Y., & Liao, H.-Y. M. (2020). *YOLOv4: Optimal Speed and Accuracy of Object Detection*. http://arxiv.org/abs/2004.10934

Bouindour, S., Hu, R., & Snoussi, H. (2019). Enhanced convolutional neural network for abnormal event detection in video streams. *Proceedings - IEEE 2nd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2019*, 172–178. https://doi.org/10.1109/AIKE.2019.00039

Feng, X., Qin, B., & Liu, T. (2018). A language-independent neural network for event detection. *Science China Information Sciences*, *61*(9), 1–12. https://doi.org/10.1007/s11432-017-9359-x

He, K., Gkioxari, G., Dollár, P., & Girshick, R. (2020). Mask R-CNN. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *42*(2), 386–397. https://doi.org/10.1109/TPAMI.2018.2844175

Kuznetsova, A., Rom, H., Alldrin, N., Uijlings, J., Krasin, I., Pont-Tuset, J., Kamali, S., Popov, S., Malloci, M., Kolesnikov, A., Duerig, T., & Ferrari, V. (2018). The Open Images Dataset V4: Unified image classification, object detection, and visual relationship detection at scale. *International Journal of Computer Vision*, *128*(7), 1956–1981. https://doi.org/10.1007/s11263-020-01316-z

Lin, T. Y., Maire, M., Belongie, S., Hays, J., Perona, P., Ramanan, D., Dollár, P., & Zitnick, C. L. (2014). Microsoft COCO: Common objects in context. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8693 LNCS*(PART 5), 740–755. https://doi.org/10.1007/978-3-319-10602-1_48

Madani, A., Boussaid, O., & Zegour, D. E. (2015). Real-time trending topics detection and description from Twitter content. *Social Network Analysis and Mining*, *5*(1), 1–13. https://doi.org/10.1007/s13278-015-0298-5

McMinn, A. J., Moshfeghi, Y., & Jose, J. M. (2013). Building a large-scale corpus for evaluating event detection on twitter. *International Conference on Information and Knowledge Management, Proceedings*, 409–418. https://doi.org/10.1145/2505515.2505695

Michaelis, S., Piatkowski, N., & Stolpe, M. (2016). Solving Large Scale Learning Tasks. Challenges and Algorithms - Essays Dedicated to Katharina Morik on the Occasion of Her 60th Birthday | Stefan Michaelis | Springer. In *Lecture Notes in Artificial Intelligence* (Vol. 9580). Springer. https://www.springer.com/gp/book/9783319417059

Nguyen, V. Q., Anh, T. N., & Yang, H.-J. (2019). Real-time event detection using recurrent neural network in social sensors. *International Journal of Distributed Sensor Networks*, *15*(6), 155014771985649. https://doi.org/10.1177/1550147719856492

Panagiotou, N., Katakis, I., & Gunopulos, D. (2016). Detecting events in online social networks: Definitions, trends and challenges. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9580*, 42–84. https://doi.org/10.1007/978-3-319-41706-6_2

Shao, S., Li, Z., Zhang, T., Peng, C., Yu, G., Zhang, X., Li, J., & Sun, J. (2019). Objects365: A large-scale, high-quality dataset for object detection. *Proceedings of the IEEE International Conference on Computer Vision*, *2019-October*, 8429–8438. https://doi.org/10.1109/ICCV.2019.00852

Shi, W., Bao, S., & Tan, D. (2019). FFESSD: An Accurate and Efficient Single-Shot Detector for Target Detection. *Applied Sciences*, *9*(20), 4276. https://doi.org/10.3390/app9204276

Tan, M., Pang, R., & Le, Q. V. (2019). EfficientDet: Scalable and Efficient Object Detection. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 10778–10787. http://arxiv.org/abs/1911.09070

Wang, C. Y., Mark Liao, H. Y., Wu, Y. H., Chen, P. Y., Hsieh, J. W., & Yeh, I. H. (2020). CSPNet: A new backbone

that can enhance learning capability of CNN. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, *2020-June*, 1571–1580. https://doi.org/10.1109/CVPRW50498.2020.00203

Yu, F., Chen, H., Wang, X., Xian, W., Chen, Y., Liu, F., Madhavan, V., & Darrell, T. (2018). BDD100K: A Diverse Driving Dataset for Heterogeneous Multitask Learning. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2633–2642. http://arxiv.org/abs/1805.04687