ALIGNER

ALIGNER D2.3

Policy recommendations

Deliverable No.	D2.3
Work Package	WP2
Dissemination Level	PU
Author(s)	Lindsay Clutterbuck (CBRNE)
Co-Author(s)	Richard Warnes (CBRNE) Irina Marsh (CBRNE)
Contributor(s)	-
Due date	2022-09-30
Actual submission date	2022-09-29
Status	Final
Revision	1.0
Reviewed by (if applicable)	Donatella Casaburo (KUL), Daniel Lückerath (Fraunhofer) Ari Basen (SIEAB), Marco Filippi (SIEAB), Karl Hertting (LEAAB)

This document has been prepared in the framework of the European project ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101020574.

The sole responsibility for the content of this publication lies with the authors. It does not necessarily represent the opinion of the European Union. Neither the REA nor the European Commission are responsible for any use that may be made of the information contained therein.

Contact:

info@aligner-h2020.eu
www.aligner-h2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 101020574.

Executive Summary

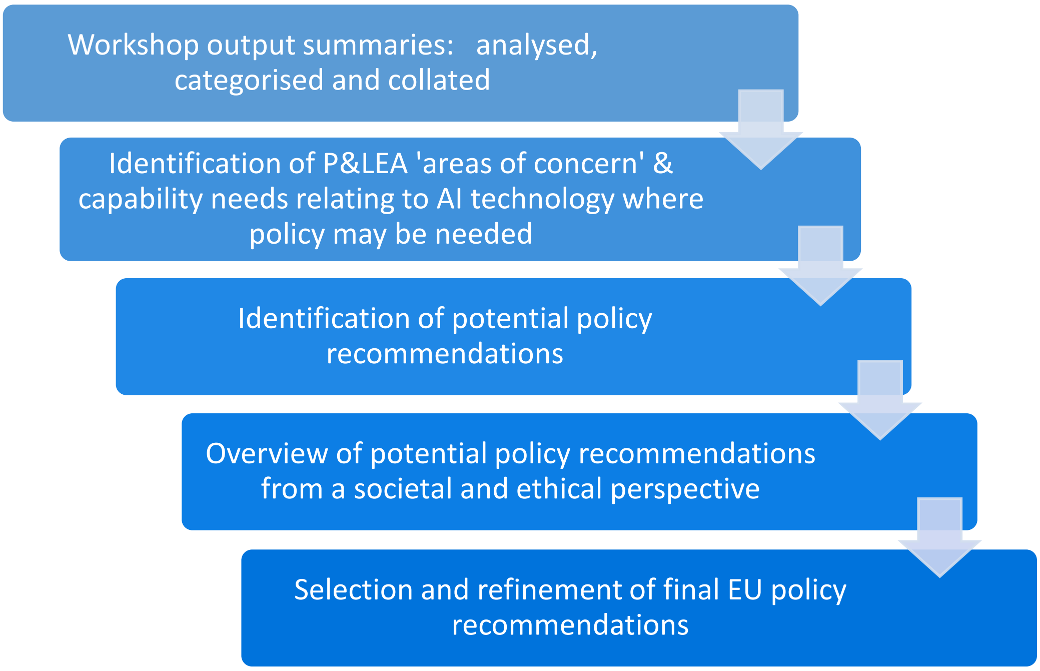
The aim of Project ALIGNER is to bring together *"…European actors concerned with Artificial Intelligence (AI), Policing and Law Enforcement and to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports LEAs while simultaneously empowering, benefiting and protecting the public."*

During the first nine months of the project three workshops were held, involving invited participants, members of the two ALIGNER Advisory Boards and representatives of other relevant EU projects, in particular projects STARLIGHT and popAI. Together, they enabled ALIGNER to explore the concept that AI technology in the context of policing and law enforcement has two dimensions; one where AI technology can be a crime and security threat and one where AI technology can be utilised by Police and Law Enforcement Agencies (P&LEA) to increase their operational capabilities and to drive improvements to their overall effectiveness.

ALIGNER has set a number of Specific Objectives (SO) and two relate specifically to the provision of the policy recommendations required for each of its three deliverables (D2.3, D2.4 and D2.5). They are required to be *"…tailored to the operational needs of the law enforcement section…supported by [identified] capability gaps…[and] provide an overview of them from a societal and ethical perspective."*[1]

To achieve this focus on P&LEA operations in the 'real world', a modified 'Grounded Theory' approach was adopted to gather and analyse the output from the workshops and to use the results to suggest policy i.e., working from the 'bottom up'. This is in contrast to a 'top down' approach where policy is created first and operational practice must then realign to comply with it. The process is shown below:

Process used to derive P&LEA Policy Recommendations from ALIGNER Workshop outputs


Workshop output summaries: analysed, categorised and collated
Identification of P&LEA 'areas of concern' & capability needs relating to AI technology where policy may be needed
Identification of potential policy recommendations
Overview of potential policy recommendations from a societal and ethical perspective
Selection and refinement of final EU policy recommendations

[1] ALIGNER Description of Work, Part B-4 and B-5

By taking into consideration all the identified 'areas of concern' and capability needs, plus the relevant elements of the wider research effort, it is possible to identify six topics where EU-led policy could have a beneficial effect in the context of policing and law enforcement. The six topics for potential EU-led policy are summarised below:

Potential EU policy recommendations to address identified P&LEA needs

1. Ensure the procurement, utilisation and in-service development of all AI technology by P&LEAs is carried out in a holistic way, with full cognizance of the adverse and beneficial impacts it may have on society
2. Ensure there is always a competent and knowledgeable 'human in the loop' if AI technology is used to support and assist P&LEAs and criminal justice systems in critical decision-making processes
3. Review the EU data protection framework on the use by AI technology of 'real-world' data as it appears to act as a barrier to the procurement and use by P&LEAs of AI technology
4. Enable and support the P&LEAs of EU Member States to bridge gaps between their current levels of technology, the AI technology of today and AI technology already on the near horizon
5. The EU should approach AI technology adoption in the context of P&LEAs and criminal justice systems by using a Directive, as used to counter terrorism from 2017 onwards
6. Conduct further and regular research into P&LEA and criminal justice concerns and capability needs for AI technology in order to ensure EU policy makers are aware of new developments and on-going issues

Overall, it is apparent that while 'AI technology' may be the cause of many of the issues identified as needing to be addressed, it is important to recognise the strong and intimate relationship that must exist between policing, law enforcement and the criminal justice systems in which they operate.

Consequently, any problematic issues arising from ethics, human rights and wider societal concerns over P&LEA utilisation of AI technology must feature at least as prominently as concerns over AI technology itself and the potential crime and security threat it can pose in the hands of hostile actors. Focusing narrowly on only this aspect, while neglecting its other dimensions, can potentially lead society into troubling areas.

Table of contents

List of Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement
KPI	Key Performance Indicator
LEEAB	Law Enforcement Agency Advisory Board (ALIGNER)
ML	Machine Learning
MO	Modus operandi
P&LEA	Policy and Law Enforcement Agencies
SIEAB	Scientific, Industrial and Ethical Advisory Board (ALIGNER)
SO	Specific Objective
TTPs	Tactics, techniques and procedures
WP	Work package

1. Introduction

Project ALIGNER commenced in October 2021, with the overall aim of *"...[bringing] together European actors concerned with Artificial Intelligence (AI), Law Enforcement and Policing to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports LEAs while simultaneously empowering, benefiting and protecting the public."*

To achieve this, ALIGNER has seven Specific Objectives (SO). Those of most direct relevance to this deliverable include requirements for:

- The formation of two project Advisory Boards (The Law Enforcement Agency Advisory Board (LEEAB) and the Scientific, Industrial and Ethical Advisory Board (SIEAB)
- A series of workshops involving experts and practitioners from the Advisory Boards, plus invited experts and practitioners and participants in other relevant EU research projects
- Based on the first three workshops, police and law enforcement agency (P&LEA) "*capability gaps*" are to be identified
- The creation of "*policy recommendations tailored to the operational needs of the law enforcement sector…[to] include operational information relating to gaps within the AI arena…whilst providing an overview…from a societal and ethical perspective"*
- The Advisory Boards will refine and agree the identified needs and policy recommendations produced for each of the three iterations of the deliverable (D2.3, D2.4, D2.5)

All of these activities take place under ALIGNER work package two (WP2), *'Law Enforcement Agencies (LEA) and Civil Society Engagement'* and occur across the three-year lifespan of the project (October 2021 to September 2024).

The aim of this deliverable, '*D2.3- Policy recommendations',* is to identify the threats, problems and issues P&LEA face using the information already gathered by ALIGNER on the current manifestations and impact of AI technology on P&LEA operations. From this information, capability gaps and 'areas of concern' have been identified, particularly those where policy may be needed to address them. These were analysed and assessed in turn to produce the six EU policy recommendations presented here.

From the initial ALIGNER workshop, an insight arose that AI technology in the context of policing and law enforcement has a dual nature. It consists of two intertwined dimensions, one where AI technology is a crime and security threat that P&LEAs must respond to and challenge when necessary, and another dimension where P&LEAs can utilise AI technology in order to carry out their functions and duties. Over the course of all the ALIGNER Workshops it became clear that in the context of policing and law enforcement, AI technology is already making an impact across these two different yet intimately interlinked dimensions.

In the 'crime and security threat' dimension, AI technology is utilised by 'bad actors' to enable them to carry out acts hostile or detrimental to society and individuals within it. Here, the key aspect for P&LEAs is that they have no control over how or why the AI technology is being used, nor (initially) over the 'bad actors' who seek to use it for their own illegal or illicit ends. This can create crime and security threats that Police and LEA's have to respond to in both the physical domain (to counter the criminals and their criminal actions) and in the digital domain (to counter the AI technology they may be utilizing to carry out their criminal actions).

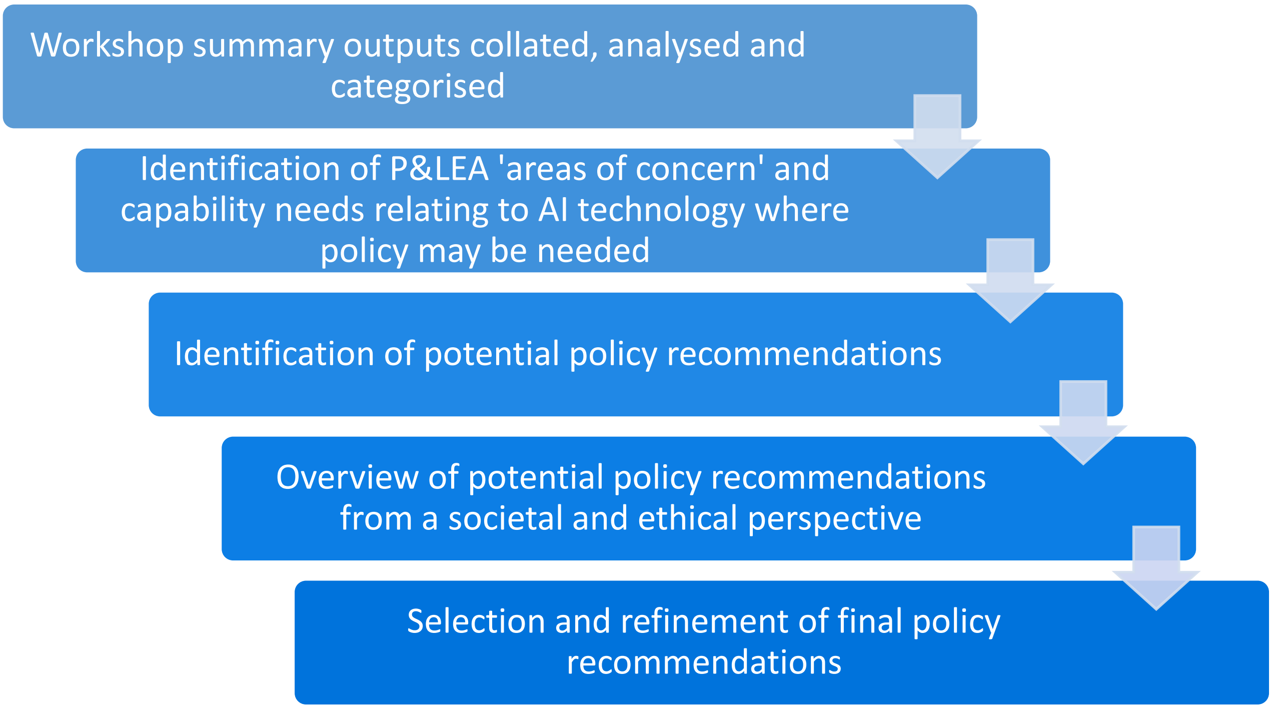
In the second of these dimensions, AI technology is utilised by P&LEAs to fulfil their duties to protect society i.e., AI technology is utilised in the service of policing and law enforcement. Here, the key aspect is that as organisations, P&LEAs are in control of the AI technology they use, from its initial deployment to its objectives and the circumstances of its use. Consequently, they can be proactive as to how it is controlled, directed and utilised. Crucially, P&LEAs are responsible and accountable for all aspects of how and why employ it and ultimately, the impact it has. A 'bad actor' using AI technology in pursuit of their criminal, hostile or malicious ends operates under no such constraints.

It is clear that ALIGNER had to approach AI technology in the context of policing and law enforcement in a holistic way if it was to achieve the most relevant and useful results. By concentrating on AI technology only as a crime and security threat, a significant gap would occur if the second critical dimension of AI technology, where it is utilised in the service of P&LEAs, is ignored or marginalised.

Section 2 of this deliverable begins the examination by briefly setting out existing EU policy measures relating to AI technology. It begins with those at a high level and with a focus on AI technology and the overall EU approach and then moves on to consider more specific policy as it relates directly to its use by P&LEAs.

Sections 3 and Section 4 describe the process of moving from the overall output from three ALIGNER workshops to the identification of a number of potential policy issues "*tailored to the operational needs of the law enforcement sector*". These are then subjected in Section 5 to an overview from a *"societal and ethical perspective*" and in Section 6, they are reviewed to explore how P&LEA needs can potentially be met (see Figure 1 below).

Figure 1 – Overview of process used to derive EU P&LEA Policy Recommendations from ALIGNER Workshop outputs



Workshop summary outputs collated, analysed and categorised

Identification of P&LEA 'areas of concern' and capability needs relating to AI technology where policy may be needed

Identification of potential policy recommendations

Overview of potential policy recommendations from a societal and ethical perspective

Selection and refinement of final policy recommendations

1.1 Gender Statement

ALIGNER partners actively safeguard gender equality and are aware of gender issues in science and technology (ref. "Commission of the European Communities: Women and Science: Excellence and Innovation–Gender Equality in Science, SEC (2005) 370, available at https://data.consilium.europa.eu/doc/document/ST-7322-2005-INIT/en/pdf).

ALIGNER monitors gender equality addressing biases and constraints throughout all the stages of the project as listed in Gendered Innovations 2 (ref "European Commission: Gendered Innovation 2 How Inclusive Analysis Contributes to Research and Innovation, (2020) available at https://op.europa.eu/en/publication-detail/-/publication/33b4c99f-2e66-11eb-b27b-01aa75ed71a1/language-en).

Outreach activities, visual representations, events, modes of data gathering and analysis, and other research products related to D2.3 have been and will be gender proofed during the internal review process following the ALIGNER Gender policy (ref: ALIGNER D1.2 Project Handbook, section 8 '*Gender aspects in publications and research*').

2. Overview of main EU policy relevant to AI technology in the context of Policing and Law Enforcement

There are two levels of EU policy that should be considered in relation to policing and law enforcement use of AI technology. First is the higher level, overarching policy framework on AI technology and its use when it relates to policing and law enforcement while secondly, there is the more specific policy level where it relates directly to P&LEA use of AI.

When examining the main EU overarching policy relevant to AI technology in the context of policing and law enforcement, there are a number of communications, updates, proposals and resolutions to consider. Most of these either support or build upon the keystone of the EU '*Proposal for a Regulation laying down harmonised rules on artificial intelligence'* (April 2021).

Widely known as the EU Artificial Intelligence Act (EU AI Act), it proposes the first ever EU legal framework on AI and aims to address and regulate its specified uses, including those for policing and law enforcement purposes. The EU AI Act takes a risk-based approach, categorizing the different uses of AI into four levels: Unacceptable Risk, High Risk, Limited Risk and Minimal Risk.[2]

In its communication document of April 2021, *'A European approach to artificial intelligence'*[3], the Commission outlined its AI package, which includes the AI Act itself, an updated review of the *'Coordinated Plan on Artificial Intelligence'*[4] and the *'Proposal for a Regulation laying down harmonised rules on artificial intelligence'*. The latter proposal contains harmonising rules which are to be passed as part of the EU AI Act. It states that *"specific restrictions and safeguards are proposed in relation to certain uses of remote biometric identification systems for the purpose of law enforcement"* and it lists the following uses of AI technology by P&LEAs:

- For making individual risk assessments
- As polygraphs and similar tools
- To detect deep fakes
- For evaluating the reliability of evidence
- For predicting the occurrence of a criminal offence
- For the profiling of persons
- For crime analytics[5]

In May 2022, the European Parliament adopted the final report of the Special Committee on Artificial Intelligence in a Digital Age (AIDA)[6], which *"aims to establish an artificial intelligence (AI) roadmap for up to 2030, with more than 150 policy recommendations on governance, data sharing, digital infrastructure, investment, e-health, e-governance, industry and security."*[7] The intent outlined in the

[2] EU, *'Proposal for a Regulation laying down harmonized rules on artificial intelligence'*, April 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

[3] EU, *'A European approach to artificial intelligence'*, Undated. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[4] EU, *'Coordinated Plan on Artificial Intelligence 2021 Review'*, 2021. https://digital-strategy.ec.europa.eu/en/policies/plan-ai#:~:text=The%20key%20aims%20of%20the,AI%20policy%20to%20avoid%20fragmentation.&text=The%20Coordinated%20Plan%20on%20Artificial%20Intelligence%202021%20Review%20is%20the,global%20leadership%20in%20trustworthy%20AI.

[5] EU, *'Annex III: High-Risk AI Systems referred to in Article 6 (2)'* in *'Proposal for a Regulation laying down harmonized rules on artificial intelligence'*, (April 2021) *Op. Cit.*

[6] EU, *'Artificial Intelligence in a Digital Age'*, 3 May 2022. https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html

[7] EU, *'Parliament proposes AI roadmap to 2030'*, 4 May 2022. https://www.dataguidance.com/news/eu-parliament-proposes-ai-roadmap-2030

document is that the EU will become a global standard-setter in AI, including its deployment and use in the field of policing and law enforcement.[8]

In addition to the higher framework level EU policy described so far, impacting on, or likely to impact on, the use of AI technology by P&LEAs, there are also more specific policy documents that directly relate to its use by P&LEA. In February 2020, the EU LIBE Committee (Civil Liberties, Justice and Home Affairs) conducted a *'Hearing on Artificial Intelligence in Criminal Law'*[9]. The hearing examined *"different questions related to the use of Artificial Intelligence in this context, such as benefits and risks of this new technology, predictive policing, facial recognition, as well as the ethical and fundamental rights implications."*[10]

Following the hearing in July 2020, the EU LIBE Committee commissioned a study on *'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights'.*[11] Along with outlining the relevant EU legal framework, this examined the use of AI technology in 'predictive policing', facial recognition, border security and its use in the wider criminal justice system. At the end of the study, the document suggested six policy recommendations:

- Assess fully the relevance and gaps of the existing legal framework
- Adapt initiatives to the specificities of the field
- Consider the need for special rules for certain practices
- Clarify the role of ethics
- Reinforce trust in EU-funded AI efforts
- Screen developments related to the Covid-19 outbreak

Perhaps the most significant EU policy in the context of policing and law enforcement, at least until the final passing of the EU AI Act and its introduction of the legal framework, is a Resolution passed in October 2021. The Resolution adopted on *'Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters'* references the previous relevant EU policy documents on various aspects of AI, most of which have already been detailed here, before noting a number of considerations in relation to the use of AI in policing and law enforcement.[12] For clarity, the relevant Resolution text is shown as a list in Figure 2 below:

Figure 2 – Uses of AI technology by P&LEAs, as per EU Resolution of October 6th, 2021

- "…In applications such as facial recognition technologies
- To search suspect databases and identify victims of human trafficking or child sexual exploitation and abuse
- Automated number plate recognition
- Speaker identification, speech identification, lip-reading technologies
- Aural surveillance (i.e., gunshot detection algorithms)
- Autonomous research and analysis of identified databases

[8] EU, *'Artificial Intelligence: MEPs want the EU to be a global standard setter'*, 3 May 2022. https://www.europarl.europa.eu/news/en/press-room/20220429IPR28228/artificial-intelligence-meps-want-the-eu-to-be-a-global-standard-setter

[9] EU LIBE Committee, *'Hearing on Artificial Intelligence in Criminal Law'*, 20 Feb 2020. https://www.europarl.europa.eu/committees/en/hearing-on-artificial-intelligence-in-cr/product-details/20200211CHE07061

[10] Ibid.

[11] EU LIBE Committee, *'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights'.* https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

[12] EU, *'Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters'.* 6 Oct 2021. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

- Forecasting (predictive policing and crime hotspot analytics)
- Behaviour detection tools
- Advanced virtual autopsy tools to help determine cause of death
- Autonomous tools to identify financial fraud and terrorist financing
- Social media monitoring (scraping and data harvesting for mining connections)
- Automated surveillance systems incorporating different detection capabilities (such as heartbeat detection and thermal cameras) …"[13]

Critically, it goes on to note that *"Whereas AI applications may offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies and judicial authorities, and combating certain types of crime more efficiently, in particular financial crime, money laundering and terrorist financing, online sexual abuse and exploitation of children as well as certain types of cybercrime… they may entail significant risks for the fundamental rights of people…".* Consequently, *"the relationship between protecting fundamental rights and effective policing must always be an essential element in the discussions on whether and how AI should be used by the law enforcement sector…"*[14]

Along with the use of AI technology by P&LEAs, the Resolution notes that, *"AI tools and applications are also used by the judiciary in several countries worldwide, including to support decisions on pre-trial detention, in sentencing, calculating probabilities for reoffending and in determining probation, online dispute resolution, case law management and the provision of facilitated access to the law…"*[15]

The resolution goes on to detail the potential ethical and human rights risks associated with police and law enforcement utilisation of AI technology, calling for transparency, human centric systems and appropriate governance and legal frameworks.

It concludes by calling for, *"comprehensive guidelines, recommendations and best practices in order to further specify the criteria and conditions for the development, use and deployment of AI applications and solutions for use by law enforcement and judicial authorities…"* and highlights the need, *"to consider whether specific legislative action on further specifying the criteria and conditions for the development, use and deployment of AI applications and solutions by law enforcement and judicial authorities is needed."*[16]

To summarise, there is a range of EU policy relevant to the use of AI technology by P&LEAs, in the form of communications, updates, studies, proposals and resolutions. These can be at the higher strategic framework level, where wider policy on AI technology also includes policing and law enforcement, or more specific EU policy documents, relating directly to the use of AI technology by P&LEAs. In the near future, these instruments are likely to be joined by binding EU legislation in the form of the EU 'Artificial Intelligence Act'.

However, this is a rapidly developing field in terms of significant AI technology advances, and consequently, the appropriate policy and legislative frameworks to support its acquisition and use by P&LEAs are still being developed and to a large degree, they are based on the groundwork contained in EU Resolution on *'Artificial Intelligence in criminal law and its use by the police and judicial authorities*

[13] Ibid
[14] Ibid.
[15] Ibid
[16] EU, *'Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters',* (Oct 21) *Op. Cit.*

in criminal matters' that was published almost a year ago in October 2021. There appears to be a risk that EU policy aimed at the 'street level' capability needs of P&LEAs may be overtaken by events in the real world or by breakthroughs in new technology or its commercial availability.

3. Police and Law Enforcement Agency (P&LEA) policy needs: Role of the ALIGNER Workshops 1-3

The aim of the first ALIGNER workshop, held at KU Leuven, University of Leuven, Belgium between November 17th and 18th, 2021 was to begin to identify 'real world' information and examples that could be utilised to devise an 'archetypical scenario' and a scenario framework relevant to the topic of AI in the context of policing and law enforcement. The participative approach adopted enabled participants to contribute their own knowledge and insights of examples, case-studies and information and to explore the issues raised.

Prior to the first ALIGNER Workshop, the research output from two other AI-focused workshops run in recent years by other entities was examined. The first of these had been held in Oxford in 2017 and was entitled "*Bad Actor Risks in Artificial Intelligence*".[17] Here, invited and in-house specialists had examined AI as a security threat across three security domains, identified as Digital Security, Physical Security and Political Security. AI technology and its specific relationship to crime and criminality was not examined. The second external workshop examined had been held under the auspices of University College London (UCL) in 2019 and was entitled "*AI and Future Crime*".[18] It had identified twenty examples of threats that together formed an *"approximate taxonomy of criminal applications"*.

At the first ALIGNER workshop, the main focus was placed on '*AI as a Crime and Security Threat*', but a start was also made on examining the other intimately connected aspect of AI technology, namely AI in the service of P&LEAs. All of the examples raised during the Oxford and London workshops were examined and discussed and this in turn generated from the ALIGNER participants new examples and ideas of AI technology as a crime and security threat.

From the resulting consolidated data, a typology of four categories and twelve sub-categories for AI as a crime and security threat was drawn up (see Annex A).[19] The workshop concluded by repeating this approach but participants were asked to concentrate on examples of where AI technology was, or was likely to be, utilised in the service of P&LEA (a theme taken up more fully during the following workshop.)

The second ALIGNER Workshop took place on-line on January 18th and 19th, 2022 and adopted the same interactive approach as in Workshop 1. It continued to examine examples of the crime and security threat posed by AI technology as examples arose but the main focus was on discussing the AI and ML 'capability enhancement needs' of P&LEAs today, their potential future needs and the actions that are required to bring AI safely and effectively into the service of P&LEA. From Workshop 2 arose a number of categories to describe where P&LEAs are utilising today, or could utilise in the future, AI technology to carry out their duties and responsibilities (see Annex A).[20]

Finally, Workshop 3 was held on June 29th and 30th in Bonn. Building on the previous workshops, it took as its central theme the issue of P&LEA capability requirements relating to AI technology. How the

[17] 'The Malicious use of Artificial Intelligence: Forecasting, prevention, and mitigation'
Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Stein- hardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. *arXiv.org*, vol. cs.AI. (2018), https://arxiv.org/pdf/1802.07228.pdf?source=post_page, Accessed October 2020

[18] 'AI-enabled future crime' M.Caldwell, J.T.Andrews, T.Tanay and L.D.Griffin, Crime Science (2020), https://link.springer.com/content/pdf/10.1186/s40163-020-00123-8.pdf, Accessed October 2020

[19] See also ALIGNER deliverable D2.2 – 'Archetypical Scenarios and their Structure', published March 31st, 2022

[20] Ibid.

outputs from all of the workshops were used to arrive at potential policy recommendations for the EU is described in the section below.

3.1 Methodology and approach

The rationale conceived prior the commencement of ALIGNER project provided a start point for the ALIGNER project work by recognising that "*Police and LEAs are at the forefront of dealing with the dual challenge of maximising the benefits of AI (for example, by benefitting from the advancement of more accurate facial recognition solutions) while simultaneously having to counter the tactics, techniques and procedures (TTPs) used to defeat the legitimate purposes of AI. To add even more complexity, the means in criminal objectives can range from legitimate, commercially available products to those that are malign and created solely for criminal purposes.*" [21]

As an integral part of ALIGNER, two expert Advisory Boards were formed early on, the Law Enforcement Agency Advisory Board (LEAAB) and the Scientific, Industrial and Ethical Advisory Board (SIEAB). Advisory Boards provided a mechanism to access the experience and technical expertise held by their members. Added to these participants were the Project consortium members and the selected participants invited to attend the workshops. Together, they ensured that the policy recommendations could be *"…tailored to the operational needs of the law enforcement sector…supported by [identified] capability gaps…[and] provide an overview of them from a societal and ethical perspective."*[22]

The research undertaken to achieve this utilised a variant of Grounded Theory and the use of data tables[23]. It provides an alternative means of analysing data other than the more traditional one built upon hypothesis, deductive theory and quantitative research. Instead, it relies on an inductive approach to the analysis of qualitative data, adapting and modifying its goal as new evidence emerges during the research process.[24]

During discussions and presentations during the first three ALIGNER Workshops, detailed notes were recorded of relevance to AI technology as a crime and security threat, AI technology in the service of P&LEAs and the existing and potential capability needs of P&LEAs. These were used to produce a detailed summary of each one. By applying an 'open coding' process to the summaries, a textual analysis the workshop activities and discussions could be conducted. This process fragmented the summaries and enabled a number of 'areas of concern' where the future development of policy may be required to be identified. To distinguish where each of the 'areas of concern' had originated from, a code was attached to each one e.g., 'WS 1' for workshop one etc.

Once these steps had been completed, the Grounded Theory process of 'axial coding' was applied to the data. This re-assembles the data that was 'fractured' during the process of 'open coding' and does so in a more meaningful and insightful way. The 'areas of concern' were then reviewed and where duplicates or overlapping aspects were found, these were amalgamated or amended to form more precise and complete summaries, each with an appropriate heading. This then became the means to

[21] ALIGNER Description of Work, Part B-10

[22] ALIGNER Description of Work, Part B-4 and B-5

[23] Grounded Theory is a methodology that uses an inductive approach to qualitative data, enabling general conclusions to be drawn out of an assembled mass of specific data points. (See Strauss, A. & Corbin, J. (1994). Grounded Theory Methodology: An Overview. In N. Denzin & Y. Lincoln *Handbook of Qualitative Research. 1st ed.* (pp 273-284) and Warnes, R. (2009) Grounded Theory. In Ling, T. & Villalba van Dijk, L. *Performance Audit Handbook: Routes to Effective Evaluation.* Santa Monica, Rand Corporation)

[24] See Glaser, B. and Strauss, A. (1967) *The Discovery of Grounded Theory: Strategies for qualitative research.* London: Transaction.

identify forty-four ‘areas of concern’ and the connections between them. In turn, they could then be grouped together into six appropriate over-arching categories. (See Annex A for full details).

3.2 Incorporating the findings from the ALIGNER Workshops

The first two ALIGNER Workshops provided specific outputs that have been utilised in the process leading to the policy recommendations. The outputs were two typologies, one based on AI technology as a crime and security threat and the other on AI technology in the service of P&LEAs. Both have been included in the Grounded Theory analysis.

3.2.1 AI technology as a Crime and Security Threat

By integrating the examples and cases discussed during the ALIGNER workshops with the two sets of inputs drawn from the external workshops held in Oxford and London[25], it was possible to construct a typology of twelve categories relevant to the ALIGNER concept of ‘AI as a Crime and Security Threat’. The ALIGNER categories are as follows:

- AI enabled fraud & forgery
- AI enabled social engineering
- AI ‘Deep Fakes’
- Weaponised autonomous drones
- Weaponised autonomous vehicles
- AI controlled robots
- AI disruption of AI systems
- AI data harvesting & exploitation
- AI disinformation & social manipulation
- Poisoned/biased AI data
- Exploitation of AI capabilities
- AI use in AI countermeasures

The twelve categories were also used to derive four, over-arching categories of ‘AI as a Crime and Security Threat’.

- AI, vehicles, robots and drones
- AI, crime and criminality in the digital age
- AI, disinformation and social manipulation
- AI and on-line cybercrime

3.2.2 AI technology in the service of Police and Law Enforcement Agencies

The approach used in ALIGNER Workshop 1 and Workshop 2 to derive the categories for ‘AI as a Crime and Security Threat’ was also taken to examine ‘AI technology in the service of P&LEAs’. However, the examples, case studies and ideas led to a different final set of categories, as seen below. The first six of them cover broad areas of P&LEA activities and capabilities. The next four are designed

[25] Oxford and UCL w/shops

to encapsulate more specifically the core functions of P&LEA where AI technology is currently, or potentially could be, beneficially applied. They are:

- Recognition and Identification of Individuals
- Crime and threat detection and prevention
- Data and information handling processes
- Digital forensics
- Digital domain activity
- Autonomous vehicles, robots and drones

- Prevention and detection capabilities
- Reaction and response capabilities
- Investigation and prosecution capabilities
- Ancillary P&LEA capabilities

The following sections of the deliverable present the results of the analysis and draw from it a number of EU potential policy recommendations.

4. Deriving potential policy recommendations from identified needs

4.1 The identified ‘areas of concern’ and their over-arching categories

Based on the analysis of all the ‘areas of concern’ arising from the workshop results, six over-arching categories were identified (See Annex A for full details). They are:

1. AI Technology: Research, development, and exploitation
2. AI technology as a Crime and Security threat
3. Legal and Judicial issues and considerations
4. Ethical and Human Rights implications of P&LEA use of AI technology
5. P&LEA utilization of AI technology to enhance and increase P&LEA capabilities
6. P&LEAs and AI technology: Internal governance and training issues

Each of the six over-arching categories are shown below, plus the headings for each of the individual ‘areas of concern’ they are based on. They are:

1. **AI Technology: Research, development, and exploitation**
   - Maximise the benefits of EU AI technology research
   - AI technology gaps between P&LEA current capabilities and future needs
   - Certification of AI technology processes, trustworthiness and security
   - AI technology in P&LEA investigations vs. Problem of ‘one size fits all’
   - Testing AI technology with real data and intelligence
   - P&LEAs to have secure ICT networks for effective AI technology use

2. **AI technology as a Crime and Security threat**
   - The crime & security threats posed by AI technology fall into four broad categories:
     - AI technology; Vehicles, robots & drones
     - AI technology; Crime & criminality in the digital domain
     - AI technology; Disinformation & social manipulation
     - AI technology; On-line cybercrime
   - A range of actors can be motivated to criminally exploit AI technology
   - Possible exploitation of AI technology for nefarious political purposes
   - AI technology as an element of Hybrid Threats
   - Detrimental impacts on business of ‘ransomware’ cyber attacks
   - AI technology use plus ‘Bots’ to drive social manipulation

3. **Legal and Judicial issues and considerations**
   - Lack of high-level legal frameworks and instruments to underpin P&LEA acquisition and utilization of AI technology
   - Legal regulations relating to P&LEA use of AI technology for task automation
   - AI as a ‘dual use’ technology: Need for appropriate legal & ‘due diligence’ checks
   - AI technology and the ‘dual use’ of ‘Chatbots’
   - AI technology generated content could undermine the integrity of Judicial systems
   - Use of AI technology assisted transcription of Court cases

- AI technology, digital forensics and digital evidence gathering

4. **Ethical and Human Rights implications of P&LEA use of AI technology**
    - Need for clear and transparent monitoring of P&LEA use of AI technology
    - AI technology and the use of the Impact Assessments (IA) to safeguard privacy and fundamental rights
    - AI technology in the Commercial and Business world: The need for checks and balances
    - Public trust in AI technology generated data

5. **P&LEA utilisation of AI technology to enhance P&LEA capabilities**
    - The utilisation (or potential utilisation) of AI technology by P&LEAs falls into ten categories:
        - Recognition and identification of individuals
        - Crime and threats; their detection and prevention
        - Data and information handling processes
        - Digital forensics
        - Digital domain activity
        - Autonomous vehicles, robots and drones
        - Preventive and detection capabilities
        - Reactive and response capabilities
        - Investigative and prosecutorial capabilities
        - Other ancillary P&LEA capabilities
    - Public acceptance of P&LEAs using AI technology in the virtual world
    - P&LEA use of AI technology to detect 'hate speech' and behavioural indicators
    - P&LEA use of AI technology in vehicles, robots and drones
    - P&LEA use of AI technology for predictive purposes
    - AI technology as an aid to operational decision making
    - Processing of multi-agency generated information and intelligence

6. **P&LEAs and AI technology: Internal governance and training issues**
    - P&LEA internal governance and training
    - Governance of P&LEA decision-making tools incorporating AI technology
    - Resource implications of AI technology to enhance P&LEA capabilities

4.2 Potential EU policy recommendations to address identified P&LEA needs

By taking into consideration all the identified 'areas of concern' and capability needs shown above, plus the relevant elements of the wider research effort, it is possible to identify topics where EU-led policy could have a beneficial effect from the perspective of policing and law enforcement. However, it is important to note the intimate relationship that must exist between policing, law enforcement and the criminal justice systems in which they operate.

As a consequence of this, and in addition to it, issues arising from ethics, human rights and wider societal concerns also lie at the heart of their relationship. The net result is that while 'AI technology' may be the cause of many of the 'threat' and 'in service' issues that need to be addressed, focusing narrowly on the aspect of technology and neglecting its other wider dimensions can potentially lead society into troubling areas. This aspect will be explored further in the following section.

Six topics where potential EU-led policy could assist are listed below for consideration. They fall loosely into two types, the first where the policy recommendations seem to be predominantly matters for higher EU policy to address and the second, where EU policy may be specifically required to enable and support the P&LEAs of Member States. Each policy recommendation is numbered but the number is not an indication of its priority or status.

EU Policy recommendation 1.

- ❖ *Ensure the procurement, utilisation and in-service development of all AI technology by P&LEAs is carried out in a holistic way, with full cognizance of the adverse and beneficial impacts it may have on society*
    - ▪ Treating the acquisition by P&LEAs of AI technology in the same way as other new technology is acquired and maintained is not sufficient. P&LEAs need unbiased specialist advice and guidance. In addition, they also require specialist advice and guidance on the ethical and human rights implications of their acquisition, and these must extend across the spectrum from the individual to society. The EU may be best placed to generate and disseminate this type of advice and guidance.

EU Policy recommendation 2.

- ❖ *Ensure there is always a competent and knowledgeable 'human in the loop' if AI technology is used to support and assist P&LEAs and criminal justice systems in critical decision-making processes*
    - ▪ The nature of the work carried out by P&LEAs, its impact on individuals and on wider society require that AI technology should not directly replace human decision making in the context of policing and law enforcement. Without this safeguard, all the checks and balances that are intrinsic to decision making in P&LEAs cannot occur or are compromised e.g., the fundamental issues of accountability, explicability, transparency, and compliance with the rule of law.

EU Policy recommendation 3.

- ❖ *Review the EU data protection framework on the use by AI technology of 'real-world' data as it appears to act as a barrier to the procurement and use by P&LEAs of AI technology*
    - ▪ For P&LEAs, the key question to be answered when considering the purchase of any new ICT technology tends to be "Does it work, and what will be the practical benefits?". If the capability of researchers and developers of utilising 'real' personal data to prove to interested P&LEAs that their AI technology product can deliver practical benefits in an operational P&LEA environment is diminished, then a barrier to its use is immediately raised
    - ▪ Even if the AI technology is purchased and used regardless, the data protection legislation provides for strict requirements on any on-going development or correction of the system in the light of the experience gained by the P&LEA utilising it.

EU Policy recommendation 4.

- ❖ *Enable and support the P&LEAs of EU Member States to bridge gaps between their current levels of technology, the AI technology of today and AI technology already on the near horizon. Steps to achieve this could include:*

- The creation of an 'EU Observatory' to monitor, assess, produce and circulate information, advice and guidelines relevant to the P&LEA and criminal justice systems on AI technology and how best they can utilise it as there appears to be a current need for well-founded and impartial practical guidance and advice for P&LEAs
- The use of policy to assist with EU-level guidance for Member States P&LEAs, encompassing how they can identify their AI technology needs and requirements, operate a robust procurement system to fulfil them and how they can do so in ways that do not breach their legal, ethical and societal obligations

EU Policy recommendation 5.

- ❖ *The EU should approach AI technology adoption in the context of P&LEAs and criminal justice systems by using a Directive, as used to counter terrorism from 2017 onwards*
  - The use of a legally binding EU Directive is a proven mechanism that was adopted for the purpose of combating terrorism as *"…the objectives of this Directive cannot be sufficiently achieved by the Member States but can rather, by reason of the need for Union-wide harmonized rules, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity…"*[26]

EU Policy recommendation 6.

- ❖ *Conduct further and regular research into P&LEA and criminal justice concerns and capability needs for AI technology in order to ensure EU policy makers are aware of new developments and on-going issues*
  - The topic of utilising AI technology in the context of policing, law enforcement and criminal justice systems is amorphous and complex. These difficulties are compounded by AI technology also creating potential crime and security threats that policing, law enforcement and criminal justice systems are expected to counter.
  - To find the best way forward, evidence-based research is required to better define where the main difficulties lie and to determine how they can impact on each other, with the ultimate aim of ensuring the agencies, organisations and entities whose role is to counter them are able to do so in ways that are compatible with democratic open societies.

The following section reviews from a societal and ethical perspective the 'areas of concern' identified from the data analysis and from which the EU policy recommendations have been derived.

[26] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

5. Overview of the policy recommendations from a societal and ethical perspective

As previously described, two of the Specific Objectives for ALIGNER require the creation of *"policy recommendations tailored to the operational needs of the law enforcement sector…[to] include operational information relating to gaps within the AI arena…whilst providing an overview…from a societal and ethical perspective"*. It goes on to require the overview to consider "possible impacts, benefits, advantages and disadvantages".

For the sake of clarity, this section of the deliverable concentrates on setting out an overview within the parameters outlined above. As well as the EU policy recommendations, it also includes relevant issues that have become apparent from the forty-four 'areas of concern" derived from the three ALIGNER workshops.

5.1 Introduction to the Societal and Ethical overview

A democratic society based on the 'rule of law' places great reliance on its police and law enforcement agencies. The advance of AI technology and the capabilities it can bring to the duties they are required to perform present a fundamental challenge not only to P&LEAs but to society itself.

From a historical perspective of the last two centuries, police and law enforcement agencies generally have always sought to use existing and available technologies and innovations as a means to increase and enhance their own effectiveness e.g., using the telegraph, telephone and radio for their communications, or the use of motor vehicles, computers and CCTV cameras. They also have a long track record of adapting and developing technology for their specific needs e.g., photography, fingerprinting and DNA profiling. There is no doubt that the pattern will continue with the AI technology available today and with the new developments in the future.

A constant theme running through all the 'areas of concern' identified from the analysis of the information gathered during the ALIGNER workshops are issues that have, or will have, an impact not only on society as a whole, but also the communities it contains and potentially, each individual. In four of these cases, this kind of potential impact is clear enough to group them together under the heading of *Ethical and Human Rights implications of P&LEA use of AI technology*. They are:

> *"A need for clear and transparent monitoring of P&LEA use of AI technology"*
>
> *"AI technology and the use of the Impact Assessments (IA) to safeguard privacy and fundamental rights"*
>
> *"AI technology in the Commercial and Business world: The need for checks and balances"*
>
> *"Public trust in AI technology generated data"*

However, when the remaining 'areas of concern' are examined through the lens of a "societal and ethical perspective", almost every one of them has implications of a similar nature. Some of these are more or less obvious but additionally, a number of them they are not immediately apparent. Before embarking on this task, it is of benefit to understand what a "societal and ethical perspective" should entail.

Society and AI

From an anthropological view, AI is defined as a 'techno social system', meaning that the technical characteristics of AI technology are connected to the social aspects. Social values and cultural beliefs are shaping how we design and use AI and also inform the perceptions, hopes and fears of the technologies used in everyday life.[27]

From the point of view of design and development, social values and cultural beliefs are integrated into the design. For example, data (the necessary foundation of AI technology) is deeply embedded in social and cultural values. People generate data and people decide what counts as data and how, where, when and why it should be gathered, sorted and used. From a cross-cultural perspective, a key concern is that much of the world leaves a faint digital footprint. People from low and middle- income countries are likely to be radically underrepresented in the datasets that are central to developing AI systems, reinforcing the exclusion of their interests and needs.[28]

From the point of view of implementation and use, AI technologies are entering a world that is already living, that is built on history and is shaped by cultural, economic and political structures.[29] The most thoughtfully-designed technologies can work in ways that are not 'just' because they are used in the real world with all its problems and imperfections.

Ethics and society

Ethical thinking in western societies is built on three philosophical frameworks: Virtue ethics, deontology, and consequentialism. However, formal moral frameworks have originated in all societies across the world, as well as in the context of religious frameworks, including Judaism, Christianity, and Islam, among many others. The moral frameworks drawn from philosophy and religion are important, but they form just one aspect of the wider aspects of ethics and societies.

Every culture has a living system of ethics, which also includes other factors such as history, politics, customs and law. To understand values, their cultural context must be understood. As ethics and culture are joined, ethics are not solely a philosophical abstraction and must be examined in an everyday cultural context to be fully understood.[30]

AI, Ethics, and society in the field of policing, law enforcement and criminal justice

The field of policing, law enforcement and criminal justice is particularly sensitive for the interactions between AI technology, ethics and society, as it touches upon the core relation between the individual and the State and consequently, the role of the government.[31] The AI-related developments in this field also need to be placed against the background of a progressive digital transformation of the state. The United Nations (UN) Special Rapporteur on Extreme Poverty and Human Rights described in this sense the emergence of the 'digital welfare state' in many countries across the globe, as systems of social

[27] Beer, David. "Power through the algorithm? Participatory web cultures and the technological unconscious." *New Media & Society* 11, no. 6 (2009): 985-1002

[28] World Economic Forum White Paper, "How to Prevent Discriminatory Outcomes in Machine Learning." March 12, 2018. https://www.weforum.org/whitepapers/how-to-prevent-discriminatory-outcomes-in-machine-learning

[29] Latour, Bruno. *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press, 2005

[30] Hagerty, Alexa. Rubinov, Igor. *Global AI Ethics: a review of the social impacts and ethical implications of Artificial Intelligence.* *https://arxiv.org/abs/1907.07892*

[31] Zuiderwijk, Anneke; Chen, Yu-Che; Salem, Fadi. *Implications of the use of artificial intelligence in public governance: a systematic literature review and a research agenda.* Government Information Quaterly 38 (2021) 101577. https://www.sciencedirect.com/science/article/pii/S0740624X21000137

protection and assistance are increasingly driven by technologies "used to automate, predict, identify, surveil, detect, target and punish".[32]

The rise of AI technology use in policing and law enforcement, coupled with increased sophistication of AI applications, continues to raise many ethical and societal concerns for law enforcement worldwide. Examples include societal concerns related to privacy, safety, risk, and threats,33 social and ethical dilemmas about fairness, bias, and inclusion[34] and governance questions related to transparency, regulatory frameworks and representativeness.[35]

The ethical and public governance questions raised by P&LEA use of AI technology are also intermingled with complex "wicked problems"[36] faced by governments, with rising perceptions of threat by societies and digital era political turbulence, where AI is taking the central stage. The use of AI has various challenges unique to the public sector[37] which significantly impact on the law enforcement field as well:

- the requirement that AI adoption in the public sector advances the public good
- the use of AI in the public sector should be as transparent as possible to gain citizens' confidence in the AI application and to ensure that their trust is deserved and retained
- the need for "regular scrutiny and oversight that is generally not seen in the private sector"
- a diverse set of stakeholders is involved, and these may have conflicting interests and agendas that add further complexity

Many of the concerns mentioned above call for better governance structures, including policy development at a governmental level.

In the light of all these considerations, the 'areas of concern' and any potential policy recommendations that are drawn from them are next considered in two ways. First, to examine the advantages and benefits that the suggested measures can bring to a society if their introduction is compliant with its underlying set of moral principles. Second, to expand the examination to take full account of the obvious, inherent and potential impacts and disadvantages of introducing them.

[32] A/HCR/41/39 United Nation-Human Right Council (2019). Special Rapporteur on Extreme Poverty and Human Rights: Climate change and poverty, apud European Parliament LIBE Committee. *Artificial Intelligence and Law Enforcement.* 2020

[33] Yudkowsky, E. (2008). Artificial intelligence as a positive and negative factor in global risk. In N. Bostrom, & M. M. Ćirković (Eds.)*, vol. 1. Global catastrophic risks* (p. 184). New York: Oxford University Press.

[34] International Labour Organization. (2019). *Work for a brighter future – global commission on the future of work*, https://www.ilo.org/global/publications/books/WCMS_662410/lang--en/index.htm apud Zuiderwijk, Anneke; Chen, Yu-Che; Salem, Fadi. *Implications of the use of artificial intelligence in public governance: a systematic literature review and a research agenda.* Government Information Quaterly 38 (2021) 101577.

[35] OECD. (2019b). *Recommendation of the council on artificial intelligence.* https://www.fsmb.org/siteassets/artificial-intelligence/pdfs/oecd-recommendation-on-ai-en.pdf

[36] Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge Handbook of Artificial Intelligence, 1*, 316–334.

[37] Zuiderwijk, A.; Chen., C; Salem, F. *Implications of the use of artificial intelligence in public governance: a systematic literature review and a research agenda.* Government Information Quaterly 38 (2021) 101577. https://www.sciencedirect.com/science/article/pii/S0740624X21000137

5.2 Potential policy recommendations: Advantages and benefits

In this section, the main potential benefits of P&LEAs utilising AI for policing and law enforcement are set out, as identified in a systematic literature review by Zuiderwijk et al[38] and complemented by the analysis set out in full in Annex A. Each review category below includes an example and a reference to its location in Annex A. Benefits were identified across nine categories:

1) Efficiency and performance benefits
2) Risk identification and monitoring benefits
3) Economic benefits
4) Data and information processing benefits
5) Service benefits
6) Benefits for society at large
7) Decision-making benefits

1. Efficiency and performance benefits refer to enhancing law enforcement operational efficiency and e-government services and systems (as in border control). For example, efficiency is improved by automating processes and tasks or by simplifying processes using Machine Learning (ML).[39] Using AI technology in policing and law enforcement also offers opportunities to resource-constrained organizations to minimise repetitive tasks. However, increased efficiency at one point in a system can generate bottlenecks elsewhere if the system as a whole is not upgraded to cope with it.

   Example – 'P&LEA utilization of AI technology to enhance P&LEA capabilities', specifically 'Data and information handling processes'
   (Annex A, Category 5)

2. Risk identification through the monitoring of potential problematic concerns can be more effective by using AI technology. For instance, P&LEAs can use AI technology to increase monitoring of urban locations to improve crime detection and crime prevention

   Example - 'P&LEA utilization of AI technology to enhance P&LEA capabilities', specifically, 'Crime and threats; their detection and prevention' and sub-category 'P&LEA use of AI technology for predictive purposes'
   (Annex A, Category 5)

3. AI technology for policing and law enforcement potentially leads to economic benefits, such as making e-government services and systems more economical by reducing costs through work-force substitution.[40]

[38] Ibid.

[39] Alexopoulos, C., Lachana, Z., Androutsopoulou, A., Diamantopoulou, V., Charalabidis, Y., & Loutsaris, M. A. (2019). How machine learning is changing e- government. In *Paper presented at the 12th international conference on theory and practice of electronic governance, Melbourne, Australia*

[40] Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review, 21*(7), 1076–1100.

Example - 'AI Technology: Research, development and exploitation', specifically the sub-category 'Maximise the benefits of previous, current and future EU AI technology research'
(Annex A, Category 1)

4. Data and information processing benefits can accrue by processing large amounts of data in over short timescales. By using AI technology, so-called 'big data' can be processed without human intervention. It can be used to establish intelligent networks that model, analyse, and use data for prediction in real-time.[41]

   Example - 'P&LEA utilization of AI technology to enhance P&LEA capabilities', specifically, 'Data and information handling processes' and the sub-category of 'Processing of multi-agency generated information and intelligence'
   (Annex A, Category 5)

5. Service benefits can be attained by improving the quality of public services as well as by reducing service time and increasing productivity.

   Example - 'AI Technology: Research, development and exploitation', specifically the sub-Category 'Maximise the benefits of previous, current and future EU AI technology research'
   (Annex A, Category 1)

6. AI technology use in policing and law enforcement leads to benefits for society at large and generates public value, for instance, by improving the ability of government to serve the population and by improving people's quality of life (more safety, less crime). At an operational level it can address problems such as a shortage of resources and the ability to more accurately scale operations.[42]

   Example - 'P&LEA utilisation of AI technology to enhance P&LEA capabilities' (various)
   (Annex A, Category 5)

7. Decision-making benefits, where Machine Learning (ML) could support P&LEA decision-makers in an operational setting and lead to better and more accurate decision-making under pressures of time and limited resources.[43]

   Example - 'P&LEA utilization of AI technology to enhance P&LEA capabilities', Sub-Category 'AI technology as an aid to operational decision making')
   (Annex A, Category 5)

[41] Ben Rjab, A., & Mellouli, S. (2018). Smart cities in the era of artificial intelligence and internet of things: literature review from 1990 to 2017. In *Paper presented at the 19th annual international conference on digital government research: Governance in the data age, Delft, the Netherlands*.

[42] Valle-Cruz, D., Alejandro Ruvalcaba-Gomez, E., Sandoval-Almazan, R., & Ignacio Criado, J. (2019). *A review of artificial intelligence in government and its potential from a public policy perspective. In Paper presented at the 20th annual international conference on digital government research, Dubai, United Arab Emirates.*

[43] Alexopoulos, C., Lachana, Z., Androutsopoulou, A., Diamantopoulou, V., Charalabidis, Y., & Loutsaris, M. A. (2019). How machine learning is changing e- government. In *Paper presented at the 12th international conference on theory and practice of electronic governance, Melbourne, Australia*

The potential advantages and benefits that the use of AI technology by P&LEA could bring are not without their dangers. They have within themselves the potential to impact negatively on society, while simultaneously being introduced with the intention of producing positive impacts. For instance, when does the use of facial recognition technology in public places to detect and prevent crime (with its benefits to individuals and society) tip over into a mechanism that can be used for social control, or at least to become an unjustified intrusion into the life of every individual it comes into contact with? These more negative and problematic aspects of AI technology in the context of policing and law enforcement are explored below.

5.3 Potential policy recommendations: Possible impacts and disadvantages

In addition to the potential benefits of the utilisation of AI technology in policing and law enforcement, the literature analysis identified the challenges (disadvantages) and potential impacts that its use can bring. As before, they are complemented by the analysis set out in full in Annex A.

They are:

1) Data challenges
2) Organizational and managerial challenges
3) Skills challenges
4) Interpretation challenges
5) Ethical and legitimacy challenges
6) Political, legal, and policy challenges
7) Social and societal challenges
8) Economic challenges

1. Data challenges refer to challenges related to the availability and acquisition of data, the integration of data, the quality of data and the lack of structure and homogeneity. Low data quality and unclear dependencies between data and algorithms may lead to biased or skewed AI algorithm outcomes.[44]

   Example - 'AI Technology: Research, development and exploitation', specifically the sub-category 'Maximise the benefits of previous, current and future EU AI technology research'
   (Annex A, Category 1)

2. Organisational and managerial challenges include inter-agency resistance to data sharing among P&LEAs (for a variety of reasons). P&LEAs might also have a negative attitude towards risk in general and the use of AI technology in particular.[45] It appears that governments cannot

[44] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly, 37*(3), 101493.

[45] Ojo, A., Mellouli, S., & Ahmadi Zeleti, F. (2019). A realist perspective on AI-era public management. In *Paper presented at the 20th annual international conference on digital government research, Dubai United Arab Emirates*.

keep up with the rapid developments in AI technology and that the public sector lacks adequate AI governance.[46]

> *Example - 'AI Technology: Research, development and exploitation', specifically the sub-category 'AI Technology gaps between P&LEA current capabilities and future needs'*
> *(Annex A, Category 1)*

3. The challenges raised by the use of AI technology by P&LEAs can be related to their limited AI experience in-house knowledge and skills, including lack of knowledge about AI technology procurement, operation and development.[47] The absence of relevant experts and the gaps present in the technical knowledge and skills of those who are employed are also mentioned and should be addressed.

> *Example - 'P&LEA and AI technology: Internal governance and training issues', specifically the sub-category of 'P&LEA internal governance and training'.*
> *(Annex A, Category 6)*

4. Concerning the interpretation challenges, the interpretation of AI results in a law citizens and information overloads that compound this problem. Consequently, over-reliance on AI technology and AI algorithms by decision makers may lead them to make incorrect or unwise decisions. The interpretation of outcomes from AI technology systems becomes even more challenging as these systems are typically opaque, making it difficult for P&LEAs to understand the system and consequently, to communicate it within the wider criminal justice system or to publicly explain it.

> *Example – 'P&LEA utilization of AI technology to enhance P&LEA capabilities', specifically Sub-Category 'AI technology as an aid to operational decision making')*
> *(Annex A, Category 5)*

5. Ethical and legitimacy challenges concern challenges related to moral dilemmas, unethical use of data, AI technology-caused discrimination and the unethical acquisition and use of shared data. Other important themes in this category concern privacy issues, security, trust and bias.[48] Many of these ethical challenges relate to removing the human element from essential decisions.

> *Example - 'Ethical and Human Rights implications of P&LEA use of AI technology', specifically the sub-category 'AI technology and the use of Impact Assessments to safeguard privacy and fundamental rights'*
> *(Annex A, Category 4)*

[46] Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration, 43*(9), 818–829.

[47] Ibid.

[48] Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review, 21*(7), 1076–1100.

6. Political, legal, and policy challenges, where AI technology can be used in such a way that it undermines the fundamental values of due process, equal protection and transparency.[49] Since AI systems can consist of inexplicable 'black-box' processes, it is not always clear who is responsible for the criteria used by the AI or the information derived by it. In addition, questions arise over who is accountable for it and ultimately, who controls it?

   Example - 'Ethical and Human Rights implications of P&LEA use of AI technology', specifically the sub-category 'Need for clear and transparent monitoring of P&LEA use of AI technology'
   (Annex A, Category 4)

7. The social and societal challenges include the effects of AI technology on labour, mostly when the human workforce is being replaced or reduced[50] and society's unrealistic expectations concerning P&LEA use of AI technology. If these challenges are realised, they can lead to decreased social acceptance of AI.

   Example - 'Ethical and Human Rights implications of P&LEA use of AI technology', specifically the sub-category 'Public Trust in AI technology generated data'
   (Annex A, Category 4)

8. The economic challenges of AI technology use by P&LEAs refer to potential harm to the economy as a result of the technology infrastructure investments needed to enable data storage and collection.[51] Although new jobs may emerge, AI technology use in law enforcement may also eventually lead to a loss of employment, or perhaps beneficially, it may allow P&LEAs to better re-deploy their staff.

   Example - 'Ethical and Human Rights implications of P&LEA use of AI technology', specifically the sub-category 'AI technology in the Commercial and Business world: Need for checks and balances'
   (Annex A, Category 4)

Over a longer-term perspective and exacerbating all these problems is the situation that is created where faster scientific progress makes it even harder for policy makers (and P&LEAs) to keep pace with the deployment and use of new AI technologies.[52] When these technologies are especially powerful or dangerous, insufficient governance can magnify their potential for harm. This is known as the pacing problem[53] and it is an issue that technology governance already faces, for a variety of reasons shown below:

[49] Bullock, J. B. (2019). Artificial intelligence, discretion, and bureaucracy. *The American Review of Public Administration, 49*(7), 751–761.

[50] Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review, 21*(7), 1076–1100.

[51] Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review, 21*(7), 1076–1100.

[52] Clarke, S., Whittlestone, J. (2022) A survey of the Potential Long-term Impacts of AI. AIES 2022 Oxford, UK. https://arxiv.org/ftp/arxiv/papers/2206/2206.11076.pdf

[53] Marchant, G.E. (2011). The Growing Gap Between Emerging Technologies and the Law. *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem.* G.E. Marchant, B.R. Allenby, and J.R. Herkert, eds. Springer Netherlands. 19–33.

1. There are information asymmetries between the developers of new technologies and those governing them, leading to insufficient or misguided governance.
2. Big technology companies are often just better resourced than governments, especially because they can afford to pay much higher salaries to attract and retain top talent.
3. Technology interest groups often lobby to preserve aspects of the status quo that benefit them directly (e.g., subsidies, tax loopholes, protective trade measures). This makes policy change, especially with experimental policies, difficult and slow to implement.

The potential EU policy recommendations have not been subjected to a separate review of their societal and ethical dimensions. This is because they have been drawn from the 'areas of concern' and capability needs as set out above and these have already been looked at in this overview. Consequently, any conclusions that can be drawn will not be significantly different or insightful.

5.4 Direction, trends and guidance

In addition to the requirement for the policy recommendations in the deliverables to be subjected to an overview from the societal and ethical perspective, the overview is also required to *"…include direction, trends, guidance, operational information relating to gaps within the AI arena...".* The aspect of "*operational information relating to gaps within the AI arena"* has already been dealt with in Section 5 above when discussing the results of the analysis (see Annex A).

This section should briefly overview 'directions and trends' as a single element, followed by 'guidance'. However, carrying out this task in this first deliverable serves little purpose. A better approach can be adopted by using this deliverable as a baseline from which to track changes over time in the two key areas of AI technology; as a crime and security threat and P&LEA utilisation of AI technology. Only then will any meaningful 'direction, trends and guidance' be apparent and can be reviewed in the policy recommendation deliverables scheduled for September 2023 and September 2024.

6. Conclusion

The systematic analysis work carried out to produce this deliverable confirmed the existence of a number of key issues that had quickly became apparent during the ALIGNER workshops. Foremost among them are the broad scale and scope of developments in AI technology itself and its increasing potential to be used by hostile actors as a crime and security threat. Of equal importance is how, on the one hand, AI technology is already being used in the context of policing, law enforcement and criminal justice while on the other hand, how technically and organisationally challenging it is for P&LEAs to source, procure and operate AI systems. Overall, it is apparent that while the misuse of AI technology may create many of the practical issues and problems faced by P&LEAs, it may also be of great benefit to their work.

Moreover, there is another aspect of AI technology when applied in the context of policing, law enforcement and the criminal justice system as its apparently beneficial use could also lead to it becoming a risk to society if its introduction and operation is not carefully considered beforehand and then controlled and monitored in a clear and consistent way.

It is important to recognise the strong and intimate relationships that exist between policing, law enforcement and the criminal justice systems in which they operate. They are all not only interconnected but interdependent as well, hence a problem apparently solved by the use of AI technology in one place may cause its displacement to elsewhere or have other ‘downstream’ impacts.

Given the unique and central role that policing, law enforcement and criminal justice play in society, it is vital to ensure that the rights of individuals and the foundations of free societies are not undermined by the inappropriate or unconstrained adoption of AI technology.

Finally, any problematic issues arising from ethics, human rights, and wider societal concerns over P&LEA utilisation of AI technology must be treated at least as seriously as concerns over AI technology and the potential crime and security threat it can pose in the hands of hostile actors. Focusing too narrowly on the AI technology or just its operational aspects at the same time as neglecting or downplaying its other dimensions can potentially lead society into troubling areas.

The EU policy recommendations suggested here are drawn from issues that have arisen from the examination of the two dimensions of AI technology in the context of policing and law enforcement; where the deliberate misuse of AI technology by hostile or malicious actors can create crime and security threats and where AI technology can be utilised by P&LEA to serve the public good. Project ALIGNER will continue to examine both of these aspects for their potential to generate EU policy recommendations.

Annex A – Summarised and categorised ‘areas of concern’ arising from ALIGNER Workshops 1-3

Below can be found the data derived from the Grounded Theory analysis of the summarised data drawn from each of the first three ALIGNER workshops (see Section 3, ‘Methodology and Approach’ for details). The end result was forty-four ‘areas of concern’ and capability needs relating to AI technology in the context of policing and law enforcement. From these, six over-arching categories can be discerned. To ensure clarity, these six are shown below first, followed by all forty-four of the ‘areas of concern’ and capability needs. In their case, each heading is accompanied by its associated text summary. Each has been assigned to one of the six over-arching categories. The Workshop(s) where the topic arose or was discussed are indicated by a code e.g. WS 1 is Workshop 1 etc.

The six over-arching categories are:

1. AI Technology: Research, development and exploitation
2. AI technology as a Crime and Security threat
3. Legal and Judicial issues and considerations
4. Ethical and Human Rights implications of P&LEA use of AI technology
5. P&LEA utilization of AI technology to enhance and increase P&LEA capabilities
6. P&LEAs and AI technology: Internal governance and training issues

The forty-four main ‘areas of concern’ are:

1. AI Technology: Research, development and exploitation

Maximise the benefits of previous, current and future EU AI technology research (WS 1, WS 2)

Given there has been various research projects on AI technology, conducted under EU support and funding (and undoubtedly with more to come in future years), it is important to integrate and coordinate it to maximise its benefits. Currently, ALIGNER is mapping out its position in relation to relevant Horizon 2020 and Horizon Europe projects. Looking into the future, can these aims be better supported and delivered through the introduction of EC policy?

AI Technology gaps between P&LEA current capabilities and future needs (WS 1)

Any policy recommendations in relation to Police and LEA use of AI, must take into consideration the technology gap between the state of their current capabilities and their projected future capability needs and requirements.

Certification of AI technology processes, trustworthiness and security (WS 3)

Like other ‘game changing’ technological developments, innovation and advances in AI technology are increasing at an exponential rate. At the same time, there are numerous ‘high risk’ sensitivities, technical, ethical and legal, associated with the use of AI technology by P&LEA to counter criminal activities and security threats.

Given these factors, and the continually changing AI ‘landscape’ it is essential to develop ‘living’ documents and flexible policies in the areas of AI technology certification, trustworthiness and security. They should be adaptable, continually revisited and appropriately revised to keep pace with (or ideally be in advance of), emerging technological developments. Having such responsive and adaptable documents and policies will ensure that they keep up to speed with developments in AI technology and remain 'fit for purpose' rather than become quickly outdated.

However, it is important that if AI Certification is to be included, then it is not applied to the AI product itself or its technological complexity, but rather, to the *processes* used to create it and the steps taken during its development. This will assist the confidence of the police and LEAs during their 'due diligence' work before and during the purchase, deployment and employment of AI systems.

AI technology in P&LEA investigations vs. Problem of 'one size fits all' (WS 2)

AI is increasingly being used by Police & LEA to facilitate data analysis in investigations, finding connections and irregularities in a large range of heterogenous data and broadening the scope of investigation analysis. However, along with the lack of legal and operational experience, there has been a 'one size fits all' approach by P&LEAs to AI systems. To correct this perception requires an increased understanding by P&LEA of AI technology, the specialised tendering process associated with purchasing it and the parameters of its operational use.

Testing AI technology with real data and intelligence (WS 2)

One of the concerns with developing and validating effective AI technology for P&LEAs to use is the need to test technology using real data and information. This must be done in the full knowledge and understanding of the differences in European and Global AI technology validation, while ensuring there are no infringements of the GDPR or other appropriate legislation. This issue would have to be taken into careful consideration when developing current and future AI technology.

P&LEAs to have secure ICT networks for effective AI technology use (WS 2)

Given the operational criticality and sensitivity of their work, a further concern is the necessity of P&LEAs having their own secure ICT networks. This is particularly the case when dealing with time critical, large scale or mass casualty incidents. Appropriate policy recommendations for access to such ICT networks should be developed.

2. AI technology as a Crime and Security threat

Crime & security threats posed by AI technology fall into four broad categories (WS1, WS 2)

When considering threat related policy recommendations in relation to P&LEA and AI technology, it will be important to consider them in conjunction with the four overarching crime and security threat categories that have emerged to date from the work of the first two ALIGNER Workshops. These are:

- AI technology; Vehicles, robots & drones
- AI technology; Crime & criminality in the digital domain
- AI technology; Disinformation & social manipulation
- AI technology; On-line cybercrime

A range of actors can be motivated to criminally exploit AI technology (WS 1)

Policy recommendations in relation to the criminal exploitation of AI must give careful consideration to the potential ranges of criminal actors involved and their motivations for doing so. They range from lone actors with multifarious criminal and political agendas, through to Organised Crime networks, hostile States and their proxies.

Possible exploitation of AI technology for nefarious political purposes (WS 2)

Concerns were raised at the possible exploitation of AI technology for nefarious political or political agenda-driven purposes. Appropriate measures (policy, strategy, legislation etc) should be considered to counter this.

AI technology as an element of Hybrid Threats (WS 1, WS 3)

There is an increasing need to develop and utilise AI technology to identify and counter increasing levels of the 'informational' elements of Hybrid Threats, particularly where AI technology is used to enable or deliver the threat. Hybrid Threats are often State generated or State sponsored and can involve the use of Proxy Actors such as criminal networks or politically motivated individuals to disseminate disinformation and Deep Fakes and carry out cyber-attacks. Hybrid Warfare sits at the highest level of Hybrid Threat and all these elements, plus others, can be used by Hostile States as part of their military Information-Operations.

Policy is required to address these issues and when generating policy recommendations, wide-ranging consideration should be given to the issue of how potential or actual Hostile States both test and use AI technology to suppress and control their own populations (internally and externally).

Detrimental impacts on businesses of 'ransomware' cyber-attacks (WS 2)

Consideration should be given to policies relating to the potential exploitation of AI technology capabilites to counter-act or prevent 'ransomware' or other cyber/ financial crimes against business. Although P&LEA have dealt with some of the larger crime groups involved the problem is still a major one.

This is due to the relative ease of its execution, the potential criminal profits available and the fact that these crimes are often not reported by business. Small businesses, if they are subject to a 'physical' crimes or incident, they can call the police or emergency services but who can they turn to after a criminal cyber-attack? If the business pays a ransom without support, they may be committing a criminal act themselves.

AI technology use with 'Bots' to drive social manipulation (WS 2)

It is important to draw a distinction between 'misinformation' where information is wrong and inaccurate and 'disinformation' where not only is the information wrong or deliberately falsified, there is hostile or malicious intent behind its sharing or dissemination. A key concern for the future is how AI technology can be used in conjunction with 'Bots' to use disinformation carry out social manipulation. Particular concerns include the generation and spreading of disinformation by mimicking human behaviour, generating 'deep fakes' and stealing or using stolen personal identity data and information. AI technology driven ‘bots’ are already a threat in the commission of crimes such as fraud.

3. Legal and Judicial issues and considerations

Lack of high-level legal frameworks and instruments to underpin P&LEA acquisition and utilization of AI technology (WS 3)

There is a need to develop effective legal frameworks to support P&LEA utilization of AI technology, both supra-nationally and nationally. Differences between legal structures across European countries relating to AI could prove to be problematic. Any legal instruments need to be compatible, or at least acceptable, between countries, to ensure they can be used effectively across borders and jurisdictions. To achieve this, bespoke legal instruments are required while today, AI related legal instruments tend to be generalized and not very specific.

The absence of such legislation and consequent lack of legal clarity may be one of the reasons deterring P&LEAs from introducing and using AI technology.

For example, a P&LEA adducing evidence that a Court determines as inadmissible as it has been obtained unlawfully through the use of AI technology will have wasted public resources and could also result in legal criticism, reputational harm and findings of liability. Consequently, the choice for P&LEAs can either be to play ‘safe’ and not introduce or use AI technology or to take risks by using it.

Legal regulations relating to P&LEA use of AI technology for task automation (WS 2)

The future is likely to see increasing P&LEA use of AI technology for the automation of specific tasks within existing workflows. These can range from assistance to deal with multiple minor offences (volume crime) or in large-scale or complex investigations into serious crime, including terrorism.

Consequently, these developments should be in line with laws and regulations, plus determinations of the suitability and necessity of using AI for each application. Its application should be governed by factors such as the domain it is used in and the categorisation of the crimes within it.

AI as ‘dual use’ technology: Need for appropriate legal & ‘due diligence’ checks (WS1, WS2)

The workshop discussions highlighted the dual nature of AI, where it can be used in both in hostile and malicious ways by criminal and terrorist actors as well as in a beneficial way by P&LEAs. This raises the question of whether AI technology should be treated in a similar manner to ‘dual use’ technologies, such as those involving dangerous chemicals or explosive precursors? If so, lessons could be learned from experiences with them e.g. implement an awareness programme and information network amongst AI technology constructors and suppliers, develop a confidential tip off-line for concerns to be reported etc.

In terms of structures and legislation, previous work on EC projects and EU Impact Assessments focused on the security of dangerous chemicals and explosives precursors may help to develop such a framework and the legislation needed to introduce and enforce it.

AI and the 'dual use' of 'Chatbots' (WS 2)

Policy development should be considered in relation to the use of AI 'Chatbots'. These can be used to identify key words, phrases or documents across social media and, like so many uses of AI technology, this capability can be adapted and used to facilitate criminality e.g. committing cybercrime by 'grooming' people through the use of 'Chatbots'. This enables their credit card details to be obtained and then their money to be stolen.

On the other hand, AI 'Chatbots' can be used against hate speech, to help report cybercrime, or to help people interact and keep in touch on social media. AI tools to process documents and identify data streams are reliant on the integrity of assets and data. AI chatbots have been publicly released by both Microsoft (using 'Tay') and Meta (using 'BlenderBot').

AI technology generated content could undermine the integrity of Judicial systems (WS 2)

Policy needs to be developed regarding the threat posed by AI generated 'deep fakes'. These are becoming increasingly easy to produce and more difficult to detect. The concern is that it could prove difficult or impossible for Courts to formally accept digital evidence produced by any AI where it cannot be reliably shown exactly which processes and methodology the AI followed to arrive at its output.

Use of AI technology assisted transcription in Court cases (WS 3)

Policy may be required to support the introduction and use of AI technology in the recording and transcription of legal discussion and court cases. Previous work during EC Project MAGNETO could assist with such a capability. It would support the narrowing down of a mass of legal data and hence would likely help speed up processes in most country's legal systems. However, it would need to come with the condition that any assessment or decisions based on the processed transcriptions would have to have been reviewed and assessed by a legally trained human mind.

AI technology, digital forensics and digital evidence gathering (WS 2)

Twenty years ago, gathering digital evidence was possible but generally little used in mainstream P&LEA investigations. Today, the situation is very different as digital evidence can feature in almost any type of criminal investigation. Gathering, analysing and assessing digital evidence is now encompassed by the new field of 'Digital Forensics'. It encompasses Computer forensics, Mobile device forensics, Network forensics, Forensic data analysis and Database forensics and at its heart lies AI technology.

The continuing evolution of such a fundamental tool in the investigation of crime and its reliance on AI technology must surely demonstrate the need for it to be governed by well thought out and effective policies.

4. Ethical and Human Rights implications of P&LEA use of AI technology

Need for clear and transparent monitoring of P&LEA use of AI technology (WS 2)

With the use of AI technology for multi-modal data collection, data mining and analysis and its use as the basis for so-called 'predictive policing', there are concerns at the potential for infringements of human rights and freedoms. Consequently, there must be independent monitoring, combining the input of both technological and social science experts.

Transparency, integrity and accountability are critical. As part of this, there is a need for a strong peer review process based on a multi-disciplinary approach (technology and social science). This has to have transparency in its audit process and be able to demonstrate that the it uses clinical objective assessment to establish its findings. It must also be integrated with not just the P&LEAs that will use it operationally but those in the commercial sector who built, supplied and will maintain it.

AI technology and the use of the Impact Assessments (IA) to safeguard privacy and fundamental rights (WS 2)

Technological applications are rapidly advancing and there is a need to consider the impact of AI technology on human rights. Conducting Impact Assessments (IA) can help to identify harmful impacts of AI technology and its use, suggest corrections and monitor their implementation. Policy is needed to establish an effective and reliable process which has an appropriate level of transparency, specific safeguards to avoid data-driven discrimination and considers compliance with the EU Law Enforcement Directive. Any impact assessment of AI technology will need to periodically revisits the risk, hence IAs should not be a static tool but provide constant advice and input so that policy recommendations can continually evolve.

AI technology in the Commercial and Business world: Need for checks and balances (WS 2)

One area of concern (perhaps at a higher level than just AI technology in the context of policing and criminal justice) is that although AI was initially a development of academic research and therefore subject to scientific control and peer review, AI technology development is also now being driven by the commercial world and in particular, by a small number of mega-companies. As a result, there are a lack of effective checks and balances, leading to two important questions.

First, how do we maintain checks and balances on products being used in the markets and make their manufacturers responsible and accountable and second, how can commercial regulators control them and ensure a safe and equitable balance is struck?

Public Trust in AI technology generated data (WS 1)

Great care must be undertaken in protecting and maintaining public trust in the use of AI technology generated data. There are already public concerns relating to both the ‘big brother’ nature of AI, as well as the reliability and trustworthiness of data it produces or assists in producing. If such data is seen as being biased or corrupted, or is vulnerable to this occurring, it will no longer be trusted, with potentially adverse consequences for society.

5. P&LEA utilisation of AI technology to enhance P&LEA capabilities

The utilisation (or potential utilisation) of AI technology by P&LEAs falls into ten categories (WS 1, WS 2)

When considering potential policy relevant recommendations in relation to AI technology, the ten categories that have emerged from ALIGNER in relation to AI technology and its current and potential use by P&LEA should be noted. The first six cover broad areas of P&LEA activities and capabilities while the remaining four encapsulate more specific core functions that lie at the heart of many P&LEAs and where it was assessed that AI technology could be beneficially applied. They are:

- Recognition and identification of individuals
- Crime and threats; their detection and prevention
- Data and information handling processes
- Digital forensics
- Digital domain activity
- Autonomous vehicles, robots and drones

- Preventive and detection capabilities
- Reactive and response capabilities
- Investigative and prosecutorial capabilities
- Other ancillary P&LEA capabilities

Public acceptance of P&LEAs using AI technology in the virtual world (WS1, WS 3)

The virtual world, including the Dark Web, is increasingly used by hostile actors, organized criminals and terrorists. They exploit it for communications, generating funds through crypto-currencies, operating markets in illegal drugs, carrying out radicalisation and recruitment and obtaining weaponry & equipment. AI could help identify indicators such as economic and communications issues associated with terrorists and criminals using the virtual world.

The increasing adoption of AI technology by Police and LEAs must demonstrate the practical advantages they can bring to dealing with the practical, real-world problems faced by P&LEAs but equally, they must also demonstrate that it is in the wider interests of the public for this to be done and that meaningful safeguards are in place. Policy may be needed to ensure this happens.

P&LEA use of AI technology to detect 'hate speech' and behavioural indicators (WS 2)

AI can used to help identify warning indicators associated with radicalization processes. The technology can link up data across multiple fields to find and analyse radical discourses. This could be used to highlight more quickly and accurately individuals of the most concern, as well as generating insights into the driving factors at work in the radicalisation process.

P&LEA use of AI technology in vehicles, robots and drones (WS 2)

Operator remote-controlled vehicles, drones and robots already have been used by the P&LEA for a variety of reaction and response functions. These include countering improvised explosive devices (IEDs), conducting patrols and tactical surveillance, assisting in search and rescue in hazardous environments and in static or mobile guarding. Already, it is desirable that clear policies should be in place regarding their ethical deployment and use and this must become an essential requirement as AI technology is developed to enable these and other functions to be carried out autonomously.

P&LEA use of AI technology for predictive purposes (WS 2)

P&LEAs use AI technology for a range of investigative purposes. It includes the filtering, collating and analysing of a mass of data to extract potential evidence, information or intelligence that can then be utilised in so -called 'predictive policing' and to predict future crime hotspots. Clear protocols and policies should be developed to govern to their use and to avoid possible negative impacts on human rights and this must be carried out in advance of the P&LEA adoption of such methods.

AI technology as an aid to operational decision making (WS 3)

Major or critical incidents are often characterized by a mass of incoming data from multiple sources and simultaneously can be partial, confused and contradictory. AI technology can improve the utilisation by P&LEA of the systems and processes required to deliver a rapid and appropriate response to them.

However, there are social and ethical implications to the use of AI technology and ultimately, the response requires human decision making and human accountability for the actions that flow from the decisions.

Processing of multi-agency generated information and intelligence (WS 3)

There are a range of P&LEA and security organisations across not only the EU, but also more widely, in networks such as the Organisation for Security and Cooperation in Europe (OSCE). They may exist for different purposes but fundamentally they are all engaged in similar functions relating to a common aim; the collecting of data and information on terrorism and criminality to process into threat intelligence upon which decisions as to actions required can be based.

AI technology can assist in assembling and fusing information into actionable intelligence by helping to extract, process and analyse raw data. Traditionally, there have been many operational and legal barriers to the sharing of intelligence. However, its use in agreed ways by differing P&LEAs and security organisations could help to break down barriers to sharing sensitive intelligence, a particularly important objective in relation to the growing level and complexity of Hybrid Threats.

6. P&LEAs and AI technology: Internal governance & training issues

P&LEA internal governance and training (WS 2, WS 3)

As police and LEAs are becoming more involved in the use of AI technology, there is a need to develop suitable internal governance for systems utilising AI technology and for appropriate training to be delivered to the personnel who will use them. Gaps are still too likely to exist in P&LEA personnel between the operational knowledge they have of the AI technology they use and their overall awareness of relevant legal and ethical issues. The lack of training in AI ethics is particularly concerning as AI technology can often be misused in politicised situations.

There is clearly a need to raise overall capabilities, eliminate questionable uses and develop specialised cyber-crime squads. The proposed governance measures and training elements would help negate the current lack of familiarity, trust and understanding of AI technology and its uses amongst police and LEA. In addition to the introduction of relevant governance and training to the managers, supervisors and operators, wider organisational understanding should be improved by appointments of more skilled staff to key roles at senior levels.

To achieve all this, there has to be an appropriate level of education and training introduced for Police and LEA across the field of AI technology and its use, stretching from the requirements and tendering process prior to its acquisition, to how it will be maintained and upgraded and of course, how and when it will be utilized operationally.

Governance of P&LEA decision-making tools incorporating AI technology (WS 3)

With the various AI tools, especially those used by P&LEA, a clear distinction must be made between those tools which are ‘convenient’ to use and the more important decision making/decision support tools. It is critical to ensure human involvement and intervention in any decision making where AI technology plays a part and to ensure the autonomy of the individuals accountable for overseeing such decisions.

Resource implications of AI technology to enhance P&LEA capabilities (WS 3)

The presentation and ensuing workshop highlighted the increasing, and increasingly complex, level of Hybrid Threat being directed at EU Member States and others by hostile state actors and their proxies. They utilise a complex mixture of AI technology, cyber, proxy actors (including organized crime groups, terrorists, private military companies, and intelligence operators) to generate hybrid attacks across both the virtual and physical worlds.

These are aimed at undermining legal democracies, their critical infrastructure, economic wellbeing and the trust of their populations. Given this increasing threat and its associated complexity, there is a need for greater funding and increased personnel in P&LEAs and security agencies to mitigate and counter such threats. This should also extend to associated research fields, such as AI technology.