INTERPOL

unicri
United Nations
Interregional Crime and Justice
Research Institute

ARTIFICIAL INTELLIGENCE AND ROBOTICS FOR LAW ENFORCEMENT

ARTIFICIAL INTELLIGENCE AND ROBOTICS FOR LAW ENFORCEMENT

Disclaimer

The opinions, findings, and conclusions and recommendations expressed herein do not necessarily reflect the views of INTERPOL, UNICRI, or any other the national, regional or international entity involved.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

INTERPOL and UNICRI acknowledge the contribution of the experts and participants of the first Global Meeting on the Opportunities and Risks of Artificial Intelligence and Robotics for Law Enforcement held in Singapore in July 2018. In particular, the workshop was supported by the following INTERPOL and UNICRI representatives: Ms. Anita Hazenberg of INTERPOL, Mr. Irakli Beridze of UNICRI (designing of the initiative and overall management and moderation of the meeting); Mr. Trygve Aandstad of the National Criminal Investigation Service, Norway, formerly serving at INTERPOL (launching of the initiative); Ms. Itziar Miravalles, Mr. Han Ping Derrick Ong and Mr. Wataru Mito of INTERPOL (conceptualisation and organization of the meeting); and Mr. Kevin Anthony of INTERPOL and Mr. Odhran McCarthy of UNICRI (substantive support to the meeting and the preparation of this report). The Organizers would also like to express their appreciation to Mr. Daniel Faggella (Emerj), Mr. Thomas Campbell (FutureGrasp LLC) and Mr. James Butcher (Kairos) for their technical review of and contribution to this report.

Copyright

Viale Maestri del Lavoro,10, 10127 Torino – Italy
Tel: +39 011-6537 111 / Fax: +39 011-6313 368
Website: www.unicri.it
E-mail: unicri.publicinfo@un.org

200, Quai Charles de Gaulle, 69006 Lyon – France
Tel: +33 4 72 44 70 00 / Fax: +33 4 72 44 71 63
Website: www.interpol.int
E-mail: edgci-ic@interpol.int

FOREWORD

Artificial intelligence (AI) and robotics have taken the world by storm, seizing our collective imagination with the promise of the ability to reshape fundamental shortcomings in society. The capabilities of these technologies are advancing every day at a most remarkable pace and are even out-performing humans in certain tasks. Although films such as 'Minority Report' and 'Robocop' may not present the most attractive depiction of the future of advanced technologies in law enforcement, understanding how these technologies can be applied by law enforcement agencies for the safety and security of our global community is of critical importance.

It is already well established that criminal groups are not reticent about exploiting technology, having, for instance, capitalised on mobile phones and global positioning system (GPS) devices from their earliest days and, more recently, turning to the dark web and cryptocurrencies and exploiting cyber vulnerabilities. Crime has gone high-tech and we are likely to see criminal groups continue to adapt to and employ the latest technologies to their benefit. As AI and robotics evolve and become more dispersed throughout society, new threats and crimes related to their malicious use will emerge. Law enforcement must be ready to address these challenges and equally be prepared to leverage these technologies to better prevent and control crime.

The Innovation Centre of the International Criminal Police Organization (INTERPOL) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), which recently established a Centre for AI and Robotics, believe it is essential for law enforcement not fall behind with respect to these technologies. Through our close cooperation, our goal is to demystify the world of AI and robotics, not only for law enforcement officers, but also for policymakers, practitioners, industry partners, academic researchers and civil society.

To this end, INTERPOL and UNICRI convened a global meeting in Singapore in July 2018 on the opportunities and risks of AI and robotics for law enforcement. It provided a forum to discuss good practices in policing, current and prospective opportunities and threats, as well as ethical challenges posed by the adoption of these technologies. This report presents the main achievements of that meeting, bringing various nuanced issues to light. It is our hope that the report helps to make better sense of this challenging and dynamic area, providing thought-provoking scenarios and practical

examples. It could also serve to improve the situational awareness in law enforcement agencies across the world.

We are also pleased that the fruitful dialogue we initiated will continue later this year with the 2nd INTERPOL – UNICRI Global Meeting on Artificial Intelligence for Law Enforcement to be held as part of the INTERPOL World event from 2nd to 4th of July 2019. The second edition will aim to dive deeper into some of the issues raised during the first meeting, specifically on the ethically responsible integration of AI and machine learning in law enforcement to capture and evaluate data and the practical experiments and projects being implemented.

The path ahead is a long one, but it is possible to develop our understanding and collective capabilities by working together to test traditional boundaries and tackle difficult ethical questions, if we are well prepared, the future of AI and robotics in law enforcement will be empowerment, contributing to peace, stability and security for communities to flourish.

Anita Hazenberg
Director, INTERPOL's Innovation Centre

Irakli Beridze
Head, UNICRI Centre for AI and Robotics

EXECUTIVE SUMMARY

The first Global Meeting on the Opportunities and Risks of Artificial Intelligence (AI) and Robotics for Law Enforcement was organized by INTERPOL's Innovation Centre and the United Nations Interregional Crime and Justice Research Institute (UNICRI), through its Centre for Artificial Intelligence and Robotics, and took place in Singapore on 11 and 12 July 2018.

Participants of this first meeting were actively involved in presentations on insights and foresight of AI and robotics, three open discussions (break-out) sessions, and six live demonstrations of the latest innovations and new technologies in the application of AI and robotics.

The key findings of this meeting were:

1. AI and robotics are new concepts for law enforcement and there are expertise gaps which should be filled to avoid law enforcement falling behind.

2. Many countries are exploring the application of AI and robotics in the context of law enforcement. Some countries have explored further than others and a variety of AI techniques are materializing according to different national law enforcement priorities. There is, however, a need for greater international coordination on this issue.

3. In general, the law enforcement community is modest about its national capacities but is eager to develop its experience and capabilities.

4. Some interesting examples of AI and robotic use cases for law enforcement include:

    a. Autonomously research, analyze and respond to requests for international mutual legal assistance
    b. Advanced virtual autopsy tools to help determine the cause of death
    c. Autonomous robotic patrol systems
    d. Forecasting where and what type of crimes are likely to occur (predictive policing and crime hotspot analytics) in order to optimize law enforcement resources
    e. Computer vision software to identify stolen cars
    f. Tools that identify vulnerable and exploited children
    g. Behaviour detection tools to identify shoplifters
    h. Fully autonomous tools to identify and fine online scammers
    i. Crypto-based packet tracing tools enabling law enforcement to tackle security without invading privacy.

5. Several use cases in law enforcement are already in different stages of development. Some are still in a concept stage, while others are in prototyping, evaluation, or already approved for use.

6. AI and robotics will significantly enhance law enforcement's surveillance capabilities and, as this occurs, it will be necessary to address privacy concerns associated with these technologies, including issues such as when and where it is permissible to use sensors.

7. In general, discussions on the ethical use of AI and robotics need to take place, in particular as law enforcement increasingly touches upon the lives of citizens. Law enforcement should take steps to ensure fairness, accountability, transparency and that the use of AI and robotics is effectively communicated to communities.

8. It is also important to advance understanding of and prepare for the risk of malicious use of AI by criminal and terrorist groups, including new digital, physical, and political attacks. Possible malicious uses include AI-powered cyber-attacks, proliferation of fake news, as well as face-swapping and spoofing tools that manipulate video and endanger trust in political figures or call into question the validity of evidence presented in court.

9. The social impact of using AI and robotics in law enforcement is also high and it is advisable to better understand what it will mean for law enforcement's perception in the communities in which they operate.

10. Law enforcement needs to continuously monitor the new technology landscape to ensure preparedness. The INTERPOL Police Technology and Innovation Radar, a world-wide overview of new, emerging technologies and their use in police practice are collected, can support in this endeavour.

11. Law enforcement agencies should dedicate time to identify, structure, categorize and share their needs in terms of AI and robotics, so as to facilitate the development of projects.

12. The future of AI and robotics is challenging. The industry is growing exponentially and innovations such as quantum computing are likely to further revolutionize the field. As an information activity based on gathering and acting upon information, AI is well-suited to contribute to enhancing law enforcement capabilities.

13. The discussion paved way for recommendations in five areas, as well as four concrete suggestions for INTERPOL Member Countries' Chiefs of Police concerning AI and robotics in the current and future policing landscape.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION:

Although the term 'Artificial Intelligence' dates back to 1955 and the notions of robots or artificially intelligent systems arguably even date back to antiquity, artificial intelligence (AI) and robotics did not truly rise to prominence until 2010s, edging their way from the realms of science fiction and an obscure academic field into the very functioning of modern society. The massive growth in computational power and increasing abundance of data that characterized the 'Digital Revolution' and the subsequent 'Information Age' have been at the core of this, vastly improving capabilities and broadening the range of real-world applications for AI and robotics. In light of this, stakeholders in both the public and private sector have begun to actively pursue these technologies with a view to revolutionizing the healthcare, automotive, financial services, transportation and logistics, communications, entertainment, retail, energy and manufacturing sectors, by enhancing efficiency, improving powers of prediction, optimizing resource allocation, reducing costs and creating new revenue opportunities.

The technological advances taking place in the fields of AI and robotics can also have many positive effects for law enforcement, for instance in terms of facilitating the identification of persons of interest or vehicles, predicting trends in criminal actions, tracking illicit flows of money, flagging and responding to fake news, and even facilitating international cooperation with INTERPOL and enhancing inter-agency communication. Nevertheless, these technologies are only tools, and a tool is only as good as its user. In the hands of criminals or terrorist groups, for instance, AI and robotics can present new digital, physical or even political threats. As these technologies become more advanced and more widely available, the potential for application by law enforcement agencies or misuse by criminals is likely to increase.

While the impact of AI and robotics on crime and security is certainly the most relevant consideration for law enforcement, it is pertinent to note that AI and robotics is a complex and highly interconnected theme, touching upon a range of other economic, legal, ethical, political, and even demographic, healthcare and environmental aspects. Maximizing the benefits and minimizing the risks of AI and robotics requires an open and comprehensive understanding of the issue and the collective engagement of a broad spectrum of stakeholders from both the public and private sector.

In this context, INTERPOL's Innovation Centre and the United Nations Interregional Crime and Justice Research Institute (UNICRI), through its Centre for Artificial Intelligence and Robotics organized the first global meeting to examine the opportunities and risks of AI and robotics for law enforcement in Singapore on 11 and 12 July. Over the course of two days, representatives from national law enforcement agencies and partners from the private sector and academia, exchanged expertise on the latest developments in the fields of AI and robotics, discussed how they can be used by law enforcement to support their activities, and took stock of potential challenges to be addressed and overcome.

This report summarizes the challenges, key findings and recommendations presented and discussed during the meeting.

2. FINDINGS:

What follows are some of the main findings that resulted from the presentations and discussions that took place over the course of the meeting.

2.1. A Double-Edged Sword

The rate of innovation in the field of AI and robotics is astounding. Recent years have seen significant advancements being made in image recognition and generation, as well as speech recognition, language comprehension and vehicle navigation. While human-level intelligence is still a distant notion, AI and robotics are already more widespread in society than is often perceived, with the technology being applied in different industries across the globe, including the healthcare, automotive, financial services, transportation and logistics, communications, entertainment, retail, energy and manufacturing sectors. In the field of law enforcement, advancements in AI and robotics can also bring both opportunities as well as risks, both of which require a strategic approach and the investment of effort and resources.

Law enforcement is an information-based activity. Information is gathered, processed and acted upon in order to prevent or control crime. For law enforcement to be effective, large quantities of information, or data, on human behavior, collected from a variety of sources are required. In this regard, AI and robotics are well-suited to transform law enforcement, by enhancing how efficiently it can acquire, analyze and act upon information.

It is even conceivable that, with the increased proliferation of sensors and growth of big data, law enforcement may become heavily dependent on AI and robotics in the near future in its fight against crime. In many criminal cases, there is already simply too much data for the traditional officers to capture and assess all relevant evidence.

How exactly can AI and robotics contribute to the future of policing? How will these technologies change the way law enforcement works? Before coming to this, it may help to first better conceptualise AI and robotics.

In computer science, AI research is understood as the study of “intelligent agents”. An intelligent agent is any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. Intelligent agency may or may not be incorporated into a programmable platform or robot. However, to avoid confusion amongst law enforcement officers and policy-makers, there is merit in

focusing, not on the technicality of AI and robotics and the complexity of the system, but rather on its functionality and usability. In this regard, discussions may benefit by drawing a simple analogy between these technologies and a car. Similar to AI and robotics, an automobile is a technical instrument that is used by law enforcement to facilitate its work. Law enforcement's transition during the early 1900's from a predominantly horse-powered force to one that relied heavily on automobiles did not require law enforcement to intimately understand the mechanics and engineering of an automobile for it get utility out of it. All that was required was to understand how it could enhance crime-fighting efforts and changed the way criminals operate.

Returning to what AI and robotics can do for law enforcement, there are, broadly speaking, four main categories for how AI and robotics can interface with cyber-physical space in the context of law enforcement: 1) Prediction and Analysis, 2) Recognition, 3) Exploration, and 4) Communication. Although there are no strict boundaries between these categories, they do have varying degrees of complexity and interaction with the environment, as indicated in Figure 1 below. The greater the degree of complexity of the system and the more chaotic the environment in which the system must operate, the more challenging the system will be to develop, prototype and integrate into law enforcement.

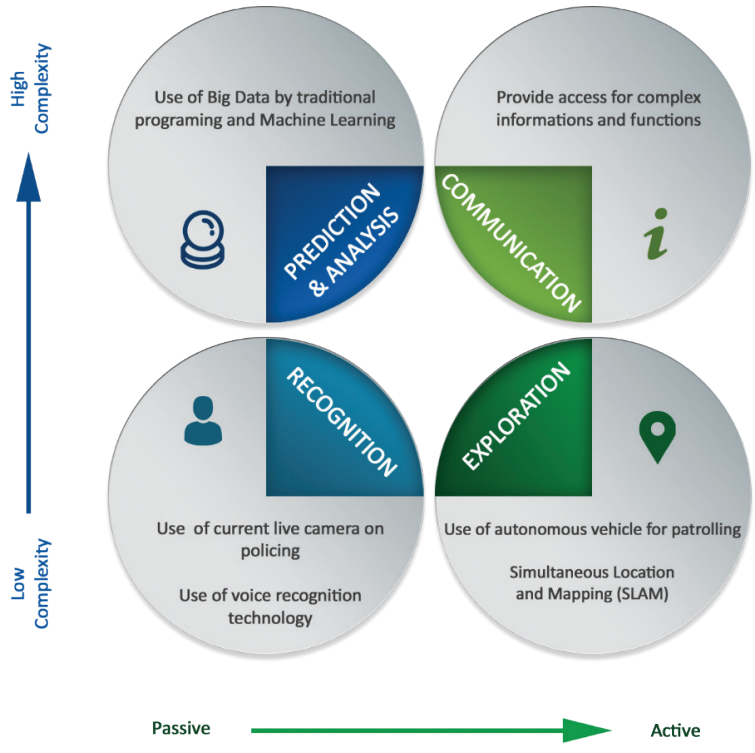


Figure 1: Four Categories of Use Cases

It should be noted, that while fully autonomous artificially intelligent systems that operate at or beyond human level intelligence may one day be a reality, discussions during the meeting indicated that the law enforcement community is, at least for now, primarily focused on narrow AI and semi-autonomous systems instruments to empower law enforcement personnel in the performance of their duties. This includes the use of systems that provide human resource savings associated with large data analysis by police in investigations.

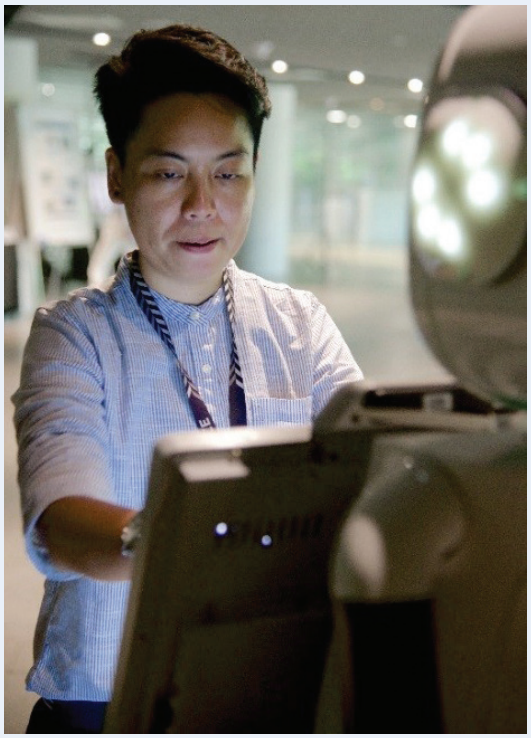
It must be emphasised that AI and robotics are very much a double-edged sword, which can lead to great changes in the way in which law enforcement approaches policing or, just as easily, enhance the modus operandi of a criminal or terrorist group or even to create entire new classes of crime altogether. A recent report by 26 authors from 14 institutions (spanning academia, civil society, and industry) investigated the issue in depth and suggested that many of the same features that might make AI and robotics appealing for law enforcement (such as scale, speed, performance, distance) might make AI and robotics equally appealing for criminals and terrorist groups.[1]

The report identifies three main domains of attack:

1. **Digital attacks,** such as automated spear phishing, automated discovery and exploitation of cyber-vulnerabilities.

2. **Political attacks,** such as the proliferation of fake news or media to generate confusion or conflict or face-swapping and spoofing tools to manipulate video and endanger trust in political figures or even result in the validity of evidence being questioned in court.

3. **Physical attacks,** such as face-recognizing armed drones or drones smuggling contraband. In the context of digital attacks, the report further notes that AI could be used either to directly carry out a harmful act or to subvert another AI system by poisoning data sets.



1 Brundage *et al.*, 2018, *The Malicious Use of Artificial Intelligence – Forecasting, Prevention, and Mitigation* (https://maliciousaireport.com/)

Although the technologies or the means to develop such technologies exist and are, to a certain degree, open-source or commercially available, AI and robotics have not played as significant a role in crime or terrorism as might be expected. While there have been instances involving such technologies, including the use of drones to land a radioactive source on the roof of the Japanese Prime Minister's office in Tokyo and by the Islamic State of Iraq and the Levant (ISIL) as unmanned aerial improvised explosive devices, the integration of such technology into crime and terrorism has not been substantially identified by law enforcement. This should not, however, be interpreted to indicate that such technologies will not be utilised for malicious purposes in the future. There is simply lack of empirical evidence on the development and use of such technologies for malicious purposes.

The weaponization of AI and robotics for criminal or terrorist purposes should however be expected to increase over time, in particular as AI and robotics become more integrated into the functioning of society and, as costs and the technical knowledge required decrease. It is therefore prudent for law enforcement to take action to forecast the nature of such future crimes and to prevent or mitigate the malicious use of AI and robotics.

2.2. Law Enforcement Use Cases

AI and robotics are new concepts for law enforcement and there are certainly expertise gaps within the law enforcement community. Notwithstanding this, many national law enforcement agencies are already actively exploring the application of AI and robotics to enhance crime prevention and control, and a broad spectrum of use cases have been or are being developed in line with national priorities on crime. Overall, the level of engagement of national law enforcement agencies in AI and robotics is far from homogenous, with some countries being more advanced than others in their exploration of these technologies. Some countries with particularly mature experience, have even established an official function within their organizations to envision AI and robotics use cases for law enforcement. Common features across the board however, are modesty with respect to national capacities and an eagerness to develop experience.

During the break-out sessions, participants were invited to share information on the practical applications being developed in their countries and to identify the stages of development – concept, prototype, evaluation, or approved for use stage. A summary of these use cases follows below.

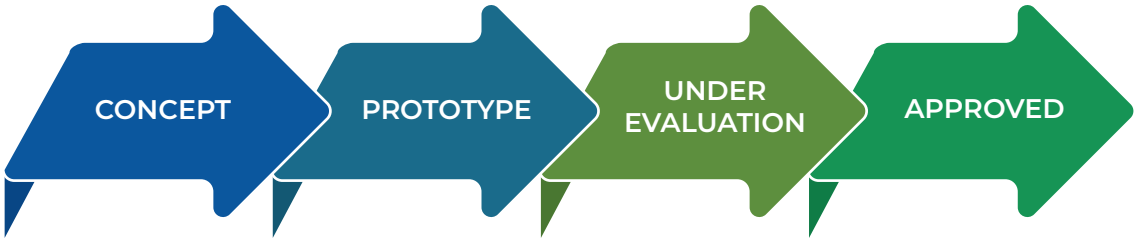


Figure 2: Stages of Development of AI and Robotics Use Cases

CONCEPT STAGE:

- AI algorithms to identify suspicious or stolen vehicles.
- Analytical tools for video and audio analysis.
- Machine learning for analysis of seized text-based media to identify potential intelligence.
- AI tools for better and more fair criminal investigations.

PROTOTYPE STAGE:

- Agent-based simulation for decision support on operations.
- Argumentation-driven information extraction to support gathering and processing of online crime reports.
- Face and soft biometrics to detect suspicious behaviour, identify criminals, and search for persons of interest.
- Contextual analysis of intelligence gathered.
- Forecasting and predicting political protests and criminal activities.
- Machine translation of audio.

- Machine learning for contextual analysis of documents to identify intent and aid officers in understanding intelligence.
- Perimeter patrol robots.
- Use of smart tools for identify child pornography.

EVALUATION STAGE:

- Predictive policing systems to support decision-makers to allocate resources.
- Patrol drones for prisons and borders.
- Audio and video analysis tools to monitor dangerous prisoners.
- Statement-taking machines to support criminal investigations.
- Scalable open digital forensics system.
- Surveillance drones.
- System to detect, tag, track and respond to suspicious persons and activities.
- Communications robots.
- Machine learning to analyse voices on telephone calls.
- Surveillance systems to monitor for and detect criminal behavior.
- AI-generated patrol live stream.

APPROVED FOR USE STAGE:

- AI bot to identify legally privileged information.
- Crime anticipation system to predict temporal and spatial features of crime thereby facilitating law enforcement to optimize its resources and ensure an effective police presence.

DEVELOPEMNT STAGE / CATEGORY OF USE				
CONCEPT	▸ Analysis of Text-based Intelligence ▸ Enhancing Fairness in Investigations	▸ Vehicle Identification ▸ Video and Audio Analysis		
PROTOTYPE	▸ Agent-Based Simulation ▸ Prediction of Protests and Crime ▸ Contextual Analysis of Intelligence	▸ Information Extraction for Online Crime Reports ▸ Face and Soft Biometrics ▸ Identification of Child Pornography	▸ Audio Translation	▸ Perimeter Patrol Robots
EVALUATION	▸ Predictive Policing ▸ Digital Forensics System ▸ Identification of Suspicious Behaviour ▸ The Incredible Machine	▸ Audio and Visual Analysis for Prisons ▸ Statement-taking Machine ▸ Voice Analysis for Telecommunications ▸ Surveillance Systems for Criminality	▸ Communication Robots	▸ Patrol Drones for Prisons and Borders ▸ Surveillance Drones ▸ AI-generated Patrol Live Stream
APPROVED FOR USE	▸ Identification of Legally Privileged Information ▸ Crime Anticipation			

▸ **Figure 3:** Result of the Use Cases Session

Of the four categories of use cases (Prediction and Analysis, Recognition, Exploration, and Communication), the most cited application of these technology was the use of AI tools for the purposes of prediction and analysis – the category of use cases that is perhaps most complex and advanced.

Beyond these use cases, a number of other possible use cases that could be explored or developed by law enforcements were presented and discussed by participants, including:

ROBOTICS APPLICATIONS

- Autonomous robots that can inspect suspicious and dangerous objects such as explosives or interact with the community using chatbots.
- Public relations robots for law enforcement agencies that can identify, greet and provide visitors with information.
- Autonomous security and surveillance using drones and 3D mapping.

DATA ANALYSIS APPLICATIONS

- Automation of processes in research, analysis and response to international mutual legal assistance requests from INTERPOL.
- Anomaly detection tools to identify suspicious financial transactions or money laundering attempts.
- Autonomous identification and fining of online scammers.

- Automation of the bureaucratic and administrative aspects of law enforcement thereby freeing officers time to deal with other tasks.
- Profiling and categorizing online identities, such as black-market buyers and sellers.
- Autonomous flagging and response to fake news or terrorist use of the internet.
- AI-based educational tools to rehabilitate and reintegrate children in the juvenile justice system and prevent recidivism.
- AI tools to identify child pornography images within data.
- Enabling law enforcement to tackle security without invading privacy via crypto-based packet tracing.

PREDICTIVE ANALYTICS APPLICATIONS

- Evaluation of risk factors and predict potential for online sexual abuse.
- Monitoring of drivers for radicalization in specific communities and predicting individuals at risk of radicalization.
- Enhancing closed circuit television (CCTV) capabilities by enabling the prediction of movement or behaviour of individuals not in a direct line of sight through the consideration of noise, vibration, and other non-visual data.

MACHINE VISION APPLICATIONS

- Advanced virtual autopsy tools to provide new insights into and to help determine cause of death.
- Behaviour detection tools that can identify shoplifters at checkouts or other suspicious activities such as loitering.
- Facial detection and validation tools that can identify criminals even through spoofing efforts and other physical elements which might be used to conceal a criminal's identity, such hats, sunglasses and beards.
- Surveillance tools that can monitor sounds, movements, and occupancy in a given room or area and detect and report anomalies.

- Recognition of a wide range of emotions in a suspect to make predictions about whether they may have been involved in a crime, as either perpetrator or witness.

- Facial validation might help law enforcement detect when a person is not who they seem or when someone has intentionally manipulated their appearance

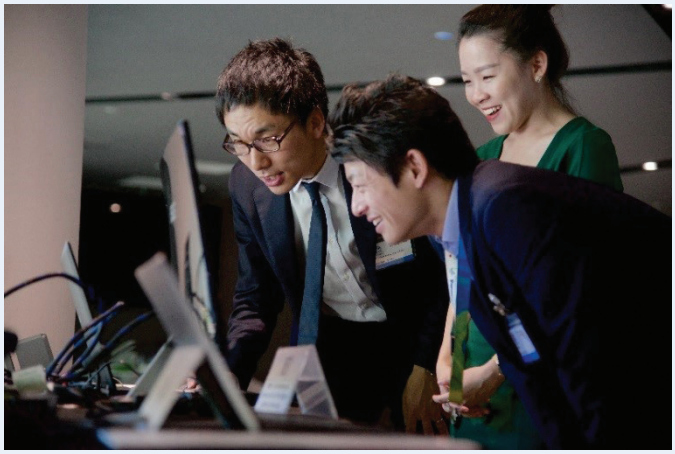
2.3. Ethics, Ethics, Ethics!

Although there is a broad spectrum of potential law enforcement use cases, a common transversal theme associated with many of these use cases is enhanced surveillance capabilities. Of course, with any type of surveillance, the potential impact on the fundamental human right to privacy as recognized by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), as well as the numerous other international and regional legal instruments, is an essential consideration. Indeed, as the use of AI and robotics by law enforcement becomes more pervasive throughout society, touching ever more upon the lives of citizens, it becomes increasingly important for law enforcement to ensure that the use of these technologies is ethical.

However, what is 'ethical' is a complex issue and largely depends on the notion of 'right and wrong', which may differ according to philosophical subscriptions or contextual variations. What is considered ethical under one set of circumstances may not be considered ethical under others. Therefore, the task of ensuring ethical use of AI and robotics in law enforcement, and other domains for that matter, is not a straightforward one.

Part of the challenge with deciphering the ethical use of AI and robotics is that law enforcement and civil society come at this from different perspectives. The primary role law enforcement is, in essence, to protect the community and its citizens from harm and, in doing so, it must find a balance between security and privacy.

Law enforcement is, at the same time, not detached from either the community or its citizens, meaning that, should it overstep its boundaries through an alleged unethical behaviour or action, it exposes itself to be held accountable by the citizens they serve. Accordingly, law enforcement must carefully consider the use of AI and robotics, in particular with respect to the placement of sensors and the usage of data collected.



To respect citizen's fundamental rights and avoid potential liability, the use of AI and robotics in law enforcement should be characterised by the following features:

Fairness: it should not breach rights, such as the right to due process, presumption of innocence, the freedom of expression, and freedom from discrimination.

Accountability: a culture of accountability must be established at an institutional and organizational level.

Transparency: the path taken by the system to arrive at a certain conclusion or decision must not be a 'black box'.

Explainability: the decisions and actions of a systems must be comprehensible to human users.

To minimise the risk that the use of these systems by law enforcement, may result in a violation of citizen's fundamental rights, a number of entities have stepped in to try to ameliorate the ambiguity of legal liability surrounding the ethical use of AI and robotics in general and to better manage political optics by advocating for 'ethics by design' in AI and robotic systems. Notably, this includes initiatives taken by the Institute of Electrical and Electronics Engineers (IEEE) to issue a global treatise regarding the Ethics of Autonomous and Intelligent Systems (*Ethically Aligned Design*), to align technologies to moral values and ethical principles.[2] The European Parliament has also proposed an advisory code of conduct for robotics engineers to guide the ethical

2 https://ethicsinaction.ieee.org/

design, production and use of robots, as well as a legal framework considering legal status to robots ("electronic personhood") to ensure certain rights and responsibilities.[3]

As these conversations on the ethical use of AI and robotics are taking place, it is important to step back and consider what it means to be human and which aspects of society should be maintained in a world with an increasing presence of AI and robotics.

Questions, such as whether society is ready for the use of facial recognition by law enforcement and the establishment of an extensive network of surveillance devices and sensors to become the norm, and to what degree society is willing to permit an increased law enforcement presence in their private lives, even if it is in the interests of public safety and security.

Law enforcement is an important test case with respect to privacy and ethics in the use of AI and robotics, predominantly because privacy is generally more likely to be trumped by security in the law enforcement community. If law enforcement can take the leadership, set norms and establish councils or bodies for the ethical use of AI and robotics, other communities may follow. Law enforcement also has the unique advantage to be discussing these issues before the use of AI and robotics becomes a common feature in law enforcement. If this opportunity is ignored and AI and robotics are used in law enforcement without fairness, accountability, transparency and explainability then the law enforcement community risks losing the confidence of the communities and citizens that it is mandated to protect.

3 http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules

3. HOW MACHINE LEARNING FOR LAW ENFORCEMENT WORKS

To avoid confusion amongst law enforcement officers and policy-makers there is merit in focusing, not on the technicality of AI and robotics and the complexity of the system, but rather on its functionality and usability. This will allow for a realistic expectation of the time, resources, and processes required in developing and implementing some of the above described use cases. The operationalization of a machine learning system can be broken down into four key phases, which are briefly described below with a set of three representative use-cases, as examples:

- Anti-money laundering.
- Theft detection in a retail store.
- Flagging suspicious social media posts.

3.1. Finding the Right Initiatives

As a first step, data scientists and law enforcement subject-matter experts must work together to discern whether or not machine learning is a viable solution for a particular problem. To do this, they must first determine how people make the decision that the system should eventually make. They must determine which parts of the decision-making process can be quantified and how to track and store those quantified parts of the decision-making process, turning them into data that might be used to train an algorithm. Should law enforcement subject-matter experts and data scientists find that the decision-making process cannot easily be quantified, then it is unlikely that machine learning will be an applicable option. Here is what this may look like for each of the three representative use cases:

Anti-money laundering: Historical transactions of thousands of clients' bank accounts are easily quantified because they are logged in each client's record, which exists within a bank's digital infrastructure. With hundreds of thousands of examples of valid and fraudulent transactions, law enforcement teams can discern the common factors (location, amount, and type of bank customer) linked to a possible criminal laundering activity. These transactions can be quantified and developed into a machine learning model.

Theft detection in a retail store: Retail stores store security camera footage in digital format, with analysis of this footage activities and actions can be quantified as data and can be used to develop a machine learning model.

Flagging suspicious social media posts: Social media posts are inherently digital containing text data, image data, post times, etc. This means that instances of suspicious or inappropriate social media posts versus benign posts are certainly quantifiable and discernible from each other. This can be developed into a machine learning model.

3.2. Labelling the Data

The only way that a machine can make a decision whether something is one thing or another, is if it ingests tens of thousands (if not millions) of examples of both options upon which it can base its decision. To facilitate this, the collected data must be labelled by the people training the system. Here is what this might look like for each of the three representative use cases:

Anti-money laundering: Historical transactions need to be labelled as either instances of money laundering or not in order for a machine to determine what makes a suspicious transaction, with known instances and their associated characteristics, the machine for all intents and purposes becomes aware of what to look for across data.

Theft detection in a retail store: Security camera footage from retail stores needs to be labelled as instances of theft or legitimate shopping.

Flagging suspicious social media posts: Social media posts need to be labelled as containing suspicious or inappropriate content or not.

3.3. Launching the Solution

Once the data is labelled, it can be fed into a machine learning algorithm. The machine learning model behind the software will then be able to make the decision the law enforcement subject-matter experts and data scientists intended for it to make. Here is what this might look like for each of the three representative use cases:

Anti-money laundering: The anti-money laundering software would be able to flag potential transactions as instances of money laundering.

Theft detection in a retail store: The system behind the security camera would be able to alert security personnel of a possible theft in progress based on the algorithm.

Flagging suspicious social media posts: The system would be able to flag social media posts as suspicious or inappropriate and alert the platform host.

3.4. Updating the Model

Launching the solution does not mean people are no longer part of the process. The model must be updated as new data is collected, and subject-matter experts must regularly assess the outputs to ensure that it is continually informed and delivering the proper results. With the volume of data that may be analyzed by the algorithm, assessments will need to be made and the model refined to improve the potential outcomes of the system. Here is what this might look like for each of the three representative use cases:

Anti-money laundering: Law enforcement subject-matter experts might inform data scientists of new methods of money laundering that criminals are adopting to deceive anti-money laundering software. They would then need to revise the process to feed new data to the algorithm so that it can detect this new kind of money laundering tactics.

Theft detection in a retail store: In cases where thieves use a novel or previously unseen method to steal items, people would need to label more footage as showing this new method of theft. That labeled data would then be used to train the algorithm to detect the new method of theft.

Flagging suspicious social media posts: People of interest to law enforcement may find new ways of communicating with each other on social media by using coded messages or phrases. Content platform employees and law enforcement officials could inform data scientists of these new methods of communication, so they can train the algorithm to identify them in social media posts.

4. MOVING FORWARD:

During the closing of the event, the focus turned towards the future, which included an overview of what may lie ahead in the future of AI and robotics, as well as a breakout session to discuss the meeting takeaways and recommendations for next steps to better prepare law enforcement for the future concerning the 'double-edged sword' of AI and robotics. A summary of these discussions follows.

4.1. Horizon Scanning

Given that AI and robotics, as evidenced by their integration into law enforcement, are already a present-day reality rather than a future possibility and that technological innovation continues to accelerate rapidly, there is merit in the law enforcement community casting an eye further into the future, to try to extrapolate potential emerging trends and technological threats and opportunities for preventing and controlling crime. Scanning the technological horizon is an important exercise to ensure that decision-makers and policy developers in the law enforcement are aware and adequately prepared for whatever the future might hold.

There have been many predictions of when these advancements will take place. Perhaps the most comprehensive predication was a survey conducted in 2015 by the Future of Humanity Institute at the University of Oxford, wherein the world's leading researchers in AI were asked when they believe AI will achieve the same quality of work for a given milestone as a human.[4] Over 1,000 experts predicted that AI will out-perform humans in some tasks, such as translating languages, driving trucks and working in retail within the next 15 years, while other, more complex, tasks may take much longer. Full automation of labour was predicted to take place in 120 years. Nevertheless, it is important to be cautious with such predictions, as it is impossible to say with any degree of certainty when they might occur.

4 Grace, *et al.*, *When will AI exceed human performance? Evidence from AI expert*, Future of Humanity Institute, University of Oxford, 2015

As noted above, the law enforcement community is, at present, looking at AI and semi-autonomous systems as instruments with a view to empowering law enforcement personnel in the performance of their duties. The potential of more advance systems to fully automate labour however, goes far beyond this, raising significant questions about the very future of law enforcement as a profession that policy makers will have to carefully consider in the years to come. At the same time, automation may also afford the opportunity to consider new perspectives to law enforcement, such as refocusing the efforts of law enforcement officers on engaging with the community and on the more social and human functions that are believed to be beyond even the most advanced machines.

Advancements in quantum computing will, for instance, help law enforcement agencies to use big data more effectively to prevent and solve crimes. Speed is the leverage that quantum computing offers AI, especially in machine learning. Quantum computing has the potential to spot patterns extremely quickly within large data sets, possibly even to access all items in a database at the same time to identify similarities in a matter of seconds. Although criminals are, unlikely to be early adopters of quantum computer, it is feasible that they will equally explore the use of these systems as part of their criminal enterprises.

There are also numerous new types of computer architectures being researched and implemented to better enable deep learning and other forms of AI. Graphics processing units (GPUs), application-specific integrated circuits (ASICs) and field-programmable gate array (FPGAs) are perhaps the most advanced new chipset technologies for AI, but there are many more. Google, Amazon, Alibaba, and many others are now developing their own proprietary chips to crunch the large volumes of data needed for deep learning.

In short, the future of AI and robotics is bright and the industry is growing exponentially, with innovations in quantum computing likely to further revolutionize the field. Law enforcement stands to benefit greatly, although steps must be taken to ensure that technological innovation does not outpace the law enforcement community. Law enforcement must endeavor to stay on top of this rapidly developing environment and will need to continuously monitor the new technology landscape to understand the impact, potential benefits of the latest technological advancements and how criminals or terrorist groups might maliciously use the very same technological advancements.

The INTERPOL Police Technology and Innovation Radar, a world-wide overview in which examples of new, emerging technologies and their use in police practice are collected, can be utilised by law enforcement agencies to support their efforts in this regard. The INTERPOL Police Innovation and Technology Radar is a tool that records and updates emerging technologies across six pillars of activities:

- Cyber, Internet and new technologies.
- Identification.
- Information processing and data analytics.
- Command, control, communication and information.
- Smart systems.
- Emerging and other technologies.

The Radar provides policing agencies worldwide the opportunity to share information and understanding of technology capabilities and to identify first adopters of new technology, connect with other likeminded agencies that are developing these capabilities. It seeks to assist in the mitigation of risks associated with planning and implementing new capabilities by those agencies. It, furthermore, provides opportunities to share lessons learned and to link leading academic, think tanks and industry partners to aid in problem identification and possible solution design.

In terms of 'Horizon Scanning' for the future of policing landscape and activities affected by emerging technologies, the Radar is a constant work-in-progress for Innovation Centre of INTERPOL and its partners. The Radar aims to ensure that policing agencies are always capable to keep up, if not become the front-runner in recognizing, addressing, and innovating the latest technologies into operative measures.

Figure 4: Current Version of Police Innovation and Technology Radar

4.2. Recommendations

The following recommendations were compiled and categorised based on information collected from participants during the third and final break-out session. The order of recommendations should not be interpreted to indicate any particular priority.

RESEARCH AND ANALYSIS:

- Law enforcement needs for AI and robotics should be identified, structured, categorized and shared to facilitate development of future projects.
- New or ongoing AI and robotics initiatives should be identified and mapped, with law enforcement agencies in Member States being informed.
- The acceptable legal and ethical boundaries for data collection & analysis for and by law enforcement should be clarified.
- Opportunities and techniques for addressing privacy and accountability issues using AI should be investigated.
- A study on "new crimes" involving the malicious use of AI and robotics should be conducted.

AWARENESS:

- Greater awareness of AI and robotics issues should be developed in law enforcement agencies through improved education and information exchange.
- The AI and robotics technology landscape should be continuously monitored.

MEETINGS AND COORDINATION:

- A forum, such as the one created during the INTERPOL-UNICRI meeting, should be kept active, through annual meetings, to facilitate further discussions on AI and robotics for law enforcement and likeminded organizations.
- International cooperation between law enforcement agencies and other relevant stakeholders should be coordinated.

- More events (meetings, training courses, and workshops) should be organized, drilling down on specific topics such as surveillance and video analytics, predictive policing, unmanned aerial vehicle deployment, ethical collection and use of data in law enforcement, AI for counter-terrorism etc.

KNOWLEDGE AND INFORMATION SHARING:

- The transfer of knowledge and experiences regarding AI and robotics throughout the law enforcement community world-wide should be facilitated.
- Relations between law enforcement, academia, industry partners and civil society should be encouraged and fostered.
- A platform for mutual cooperation, collaborative work and the sharing of expertise should be developed.

NEW TOOLS:

- There should be a greater emphasis on pilot projects to develop and test AI and robotics tools for law enforcement agencies worldwide.
- National Central Bureau in INTERPOL Member Countries should be provided with AI tools.

4.3. Suggestions for Chiefs of Police

Based on the discussions and outcomes of the meeting, the obstacles and challenges identified among others are:

- Increasing exploitation of AI by criminals in cybercrime, cyber-enabled crime, and high-tech crime.
- Difficulty in using AI to support intelligence collection and analysis to support police operations.
- Problems with conversion of sensor data to intelligence.
- Challenges in how to deploy robotics in patrolling and surveillance.
- Lack of specialization in AI of police staff.

- Insufficient awareness of products or solutions from private sector to leverage on the use of AI.
- Lack of international exchange in developing AI responses leading to duplication of efforts and waste of resources.
- Lack of translation of laws and regulations into practice concerning privacy and ethics.

Noting the obstacles and opportunities that were identified within the current and future policing landscape concerning AI and robotics, the following considerations are proposed to the Chiefs of Police:

UNDERSTAND CHALLENGES FOR LAW ENFORCEMENT AND THE NECESSITY FOR CHANGE

- Be aware of the exponential amount of information that law enforcement agencies have to handle.
- Recognize the strong international character of AI developments and criminality making use of AI.
- Verify what data is suitable for AI consumption to facilitate information sharing among law enforcement organizations and beyond.
- Understand the difficulties in integrating existing data sets into a new data dimension, in a format that can be handled by AI.
- Be prepared for new types of criminal activities exploiting AI and robotics technology.

BUILD STRATEGY AND BECOME AN AGILE ORGANIZATION

- Monitor global and national trends in the fields of AI and robotics to conduct studies on their implications in the operational environment.
- Clarify when and what part of operations require these technologies to facilitate the adoption of change.
- Assess the possibility to adopt emerging solutions.
- Experiment on how an AI application works.

- Set up a modern and up-to-date IT infrastructure involving data science environments (cluster computers) and leverage data from the operation for in-house software development.
- Build a common platform for all suitable data to be hosted with appropriate Application Programming Interfaces to access data.

INVEST IN EXPERTS AND PUBLIC-PRIVATE PARTNERSHIP

- Organize human resources policies aiming at attracting right skills and expertise.
- Encourage staff to keep anticipating future criminal activities exploiting AI.
- Create space for cybersecurity experts in the force for a better collaboration with the community.
- Create an expert group (both inside and outside of the organization) on the horizon scanning of AI used in policing and analysis of the benefit of such methods.
- Identify potential private sector partners leading in this field to collaborate with their police organizations for a better understanding of how such technologies work and how to harness them in the daily policing activities.
- Be a so-called 'smart buyer' when purchasing products and services, and where necessary develop critical functionalities.
- Invest in international exchange and joint projects and leverage on international organizations such as INTERPOL.

ENSURE ETHICAL AND LEGAL FAIRNESS AND TRANSPARENCY

- Hire AI specialists or create a unit focusing on AI not only to understand and utilize the technologies in policing but also to help set up a legal framework pertaining to AI considering ethics and privacy concerns.
- Look for ways to test new policing solutions ethically and legally. An automated analysis should be able to stand up to scrutiny by the courts or meet societal standards, norms and values.
- Study new data protection policies, such as General Data Protection Regulation in European Union, and how this effects the use of AI and big data.

ANNEX 1 TERMINOLOGY:

Understanding the opportunities and risks of AI and robotics may seem like an insurmountable challenge to a layman. A veil of confusion surrounds these subjects, which is due in part to their complex technical nature, but also to the jargon and buzzwords used in connection with AI and robotics, as well as the lack of universally accepted definitions for many of these terms. Oftentimes, terms are also used interchangeably or are used by different authors to refer to different things.

In order to help law enforcement to pierce this veil, some of the main concepts and terms that relate to the issue of AI and robotics are described below. These descriptions should not however be taken as definitions. It is beyond the scope of this report to provide a definition of these terms.

Autonomy: the freedom a system has to accomplish the goals for which it has been programmed. Autonomous systems can be either semi-autonomous, which have a human in the loop, or fully autonomous, which can perform programmed tasks without the need of any human intervention.

Artificial Intelligence: Artificial Intelligence is an intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals. The term "artificial intelligence" is applied particularly when a machine mimics "cognitive" functions that are associated with human minds, such as "learning" and "problem solving".

Artificial General Intelligence (AGI): An AI system that can perform a broad range of intellectual tasks mimicking human-level intelligence. This is also referred to as "strong AI".

Artificial Superintelligence: An AI System that can perform intellectual tasks with capabilities that far surpass those of humans.

Big Data: The massive volumes of data produced by people's digital actions, which, if harnessed and processed, can be used to improve decision-making. It is difficult to process this data using traditional database and software techniques due to the volume of the data.

Chatbot: AI-enabled communication programmes that interact with people over the internet, to provide or collect information following a pre-defined script.

Deep Learning: A method of machine learning that use a cascade of multiple layers of (deep) matrix calculation units for feature extraction and transformation. Deep Learning stands apart from other machine learning methods in that it does not require that he features of the target data be defined, instead it merely requires large amount of data and resources to process the data.

Intelligent Agent: Any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals.

Internet of Things: The network of devices connected to the Internet, including not just computational devices, such as desktops, laptops, tablets, smartphones, but also other devices containing sensors of all kinds, including devices such as activity trackers, smart thermostats, and connected cars.

Machine Learning: A computer programming technique that uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance on a specific task) from data, without being explicitly programmed.

Narrow AI: An AI system that excels at specific, very narrow tasks, but cannot perform broader, human-like, functions and, for instance, has difficulty contextualizing information.

Neural Networks: A computational network loosely inspired by biological neurons. The network consists of numerous highly interconnected processing units, each with its own respective sphere of knowledge. In response to a given input, the network adapts as needed to provide the correct output.

Robotics: A branch of engineering that focuses on the development of robots - a machine capable of carrying out a complex series of actions that can be remotely operated or autonomous. Robotics encompasses the design, construction, operation, and application of robots, as well as computer systems for their control, sensory feedback, and information processing such as AI.

Sensor: A device that detects a stimulus, such as sound, temperature, geophysical location, motion, acceleration, proximity, pressure, etc., and converts it into actionable **input for an AI or robotic system.**

Use Case: A real-world application of a specific technology.

ANNEX 2
OVERVIEW OF THE MEETING:

1. Participants

The two-day event brought together 47 participants from 20 countries. Notably, this included 25 representatives from law enforcement agencies in 13 countries in Eastern Asia, South Eastern Asia, Western Asia, Northern Europe and Oceania; 14 industry partners; 5 members of the academic community; and 3 civil society stakeholders and non-governmental organizations. Law enforcement representatives were predominantly mid-senior level and operational personnel, with varying degrees of familiarity with and understanding of AI and robotics. The majority of the participants were male, with only 5 participants being female. INTERPOL and UNICRI acknowledged that, for potential future events, the gender balance of participants should be enhanced.

Please refer to Annex 4 for the complete list of participants.

2. Objectives

Through this meeting, INTERPOL and UNICRI sought to:

- Identify and bring together global experts in AI and robotics and representatives of innovation within law enforcement agencies.
- Foster collaboration with experts in this domain from academia, industry and civil society.
- Understand the current status and future possibilities of AI and robotics use in law enforcement.
- Understand the nature of the risk of the malicious use of AI and robotics by criminals and terrorist groups.
- Share best practices in the use of AI and robotics in law enforcement.

- Explore potential interest for the establishment of a network of experts from law enforcement.
- Form durable bonds with relevant stakeholders to further develop the INTERPOL Technology and Innovation Radar.

3. Methodology

The meeting consisted of both plenary and breakout sessions. An environment of active discussion was promoted at all times and participants were encouraged to share their own experiences, best practices and lessons learned.

The meeting was formally opened, managed and moderated by the co-hosts, Ms. Anita Hazenberg, INTERPOL, and Mr. Irakli Beridze, UNICRI.

The first breakout session took place promptly after the opening of the meeting. Prior to the meeting, law enforcement representatives had been requested to prepare a poster describing a practical application of AI and/or robotics for law enforcement purposes that is being or may be developed in their respective organizations. During the first breakout session participants presented their posters. The session was organized using the World Café method, with four stations being established to allow small groups of participants to share information and discuss the use case, before the moderator called for participants to switch stations.

The second breakout session took place following the presentation of law enforcement, academia and the private sector, in which participants were invited to map use cases in their own countries that were in 1) concept, 2) prototype, 3) evaluation, or 4) approved for use stage.

A third and final breakout session took place during the closing of the meeting, where participants were invited to share their take-aways from the meeting and to propose recommendations for next steps to better prepare law enforcement for the future.

A series of live demonstration also took place over lunch on the second day, which afforded representatives of the private sector and academia the opportunity to demonstrate to their law enforcement counterparts some of the cutting-edge AI and robotics technologies and how they could benefit the law enforcement community.

Please refer to Annex III for the complete agenda.

ANNEX 3
LIST OF PARTICIPANTS:

MEMBER COUNTRIES	
Australia	Australian Federal Police
Bahrain	Ministry of Interior, NCB Bahrain
Estonia	Development Department Readiness and Response Bureau, Police and Border Guard Board
Japan	Police Info-Communications Research Center, National Police Agency of Japan
Netherlands	Dutch National Police
Norway	The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crimes
Philippines	Department of Science and Technology (DOST), Advanced Science and Technology Institute (ASTI)
Singapore	Singapore Police Force
Sweden	Swedish Defense Research Agency FOI
Turkey	Department of Information Technology, Turkish National Police
United Arab Emirates	Abu Dhabi Police
United Kingdom	National Crime Agency
Vietnam	NCB Hanoi, Ministry of Public Security of Vietnam, Institute for Strategic studies, Ministry of Public Security of Vietnam

ACADEMIA, INDUSTRY, CIVIL SOCIETY NOMINATIONS
1QBIT
AI Initiative
BootstrapLabs
Digital Asia Hub
Emerj
FutureGrasp, LLC
Future of Humanity Institute, University of Oxford
National University of Singapore
NEC
ObEN
Panasonic
SECOM
Singapore Management University
SK Telecom
Toda.Network
United Nations Office of Counter Terrorism

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in its 194 Member Countries to combat all forms of transnational crime. INTERPOL works to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Its services include targeted training, expert investigative support, specialized databases and secure police communications channels.

Located in Singapore, within the INTERPOL Global Complex for Innovation (IGCI), INTERPOL's Innovation Centre works to create strategic partnerships with law enforcement, academia and private industry on a global, regional and national level. These collaborations support INTERPOL in developing innovative solutions to policing threats and challenges.

ABOUT UNICRI

The United Nations Interregional Crime and Justice Research Institute was established in 1968. Within the broad scope of its mandate, the Institute contributes, through research, training, field activities and the collection, exchange and dissemination of information, to the formulation and implementation of improved policies in the field of crime prevention, justice and emerging security threats, due regard being paid to the integration of such policies within broader policies for socio-economic change and development, and to the protection of human rights.

In 2017, UNICRI opened its Centre for Artificial Intelligence and Robotics in The Hague, the Netherlands with a view towards advancing understanding of artificial intelligence and robotics from the perspective of crime, justice and security. The Centre seeks to share knowledge and information on the potential beneficial applications of these technologies and to contribute to addressing any potential harmful effects or their malicious use.