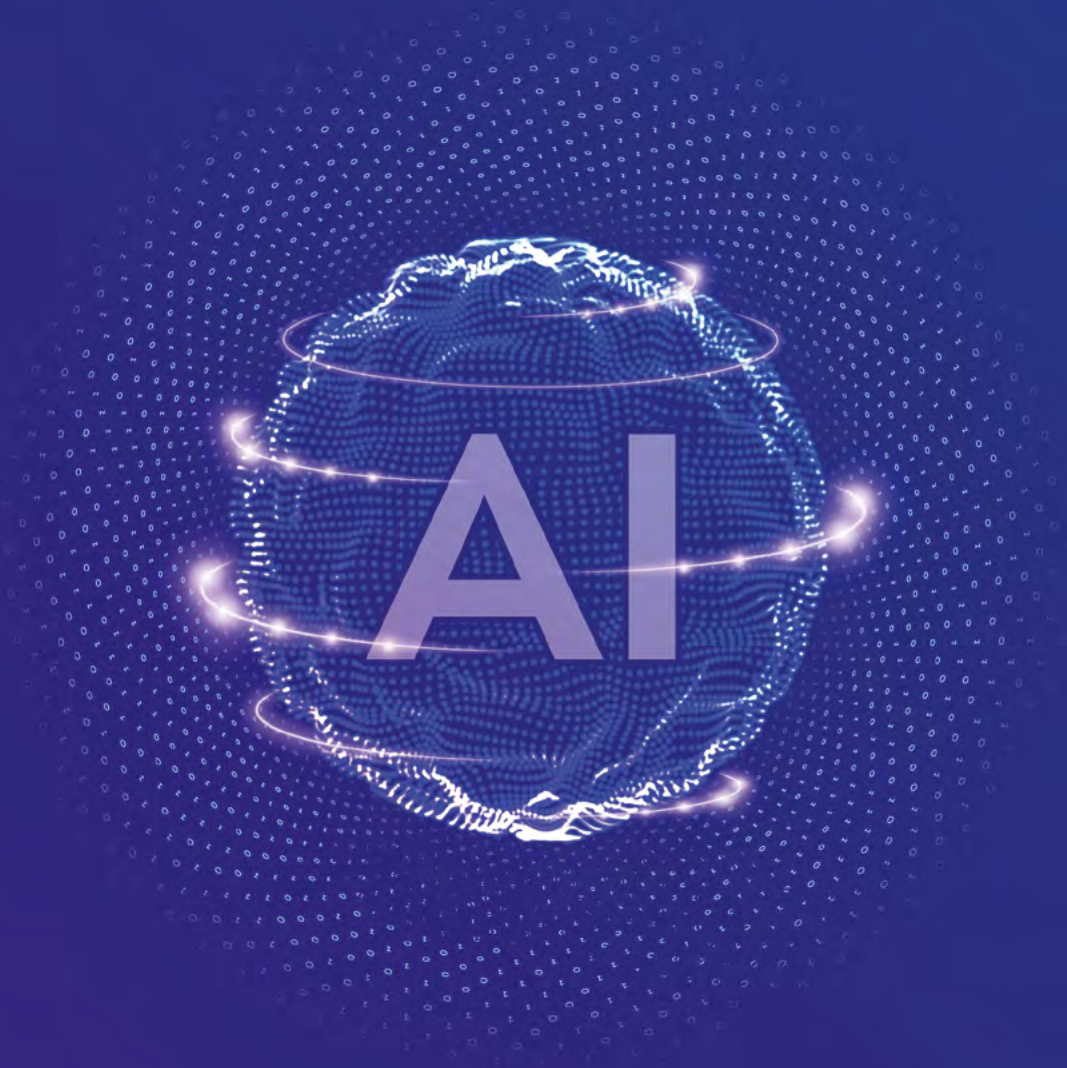
# AI in the Service of Law Enforcement - An Introduction




**NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)**
Modernization Division
**BUREAU OF POLICE RESEARCH AND DEVELOPMENT**
Ministry of Home Affairs, Government of India

# AI in the Service of Law Enforcement - An Introduction

**NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)**
Modernization Division

**BUREAU OF POLICE RESEARCH AND DEVELOPMENT**
Ministry of Home Affairs, New Delhi

*Promoting Good Practices & Standards*

*Disclaimer –*

- *This document is not a substitute for existing manuals available in the States/UTs. It is only a guide for awareness purpose. In case of any conflict, local manual/practice may prevail.*
- *BPR&D does not promote any tool/software of a particular vendor. All the tools and software mentioned in this manual are for illustration purpose only.*
- *Wherever any Image/graphics/flowchart is taken from other sources, the same has been duly acknowledged.*

**अमित शाह**

सत्यमेव जयते

**गृह मंत्री एवं सहकारिता मंत्री**
**भारत सरकार**

# संदेश

यह हर्ष का विषय है कि पुलिस अनुसंधान एवं विकास ब्यूरो द्वारा साइबर क्षेत्र में प्रौद्योगिकियों का प्रसार और उनकी संक्रमणीय चुनौतियों एवं विरोधियों द्वारा दुरुपयोग, नए खतरे के परिदृश्य और अपराधियों द्वारा किए गए तौर-तरीकों में बदलाव से निपटने के लिए निरंतर ज्ञान-निर्माण और उन्नयन की मांग करता है। राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केन्द्र (NCR&IC) इस संबंध में कानून प्रवर्तन एजेंसियों (LEAS) के लिए अनुसंधान और विकास आधारित सॉफ्टवेयर समाधान, वेबिनार, सम्मेलन, प्रशिक्षण मॉड्यूल, प्रासंगिक और प्रभावी पुस्तकों के प्रकाशन, कार्यवाही और मानक संचालन प्रक्रिया (SOPs) के रूप में विभिन्न महत्वपूर्ण पहल कर रहा है।

इन आगामी पुस्तकों का प्रकाशन **"कानून प्रवर्तन की सेवा में एआई-एक परिचय"**, **"महामारी के दौरान उभरते साइबर अपराध"**, **"फर्स्ट रिस्पॉन्डर हैंडबुक-डुअल बूट सिस्टम और नेटवर्क ड्राइव"**, **"क्लाउड इंफ्रास्ट्रक्चर से संबंधित साइबर अपराध"**, **"गूगल डैशबोर्ड डेटा का अधिग्रहण और विश्लेषण"** राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केन्द्र (NCR&IC) द्वारा इस संबंध में एक प्रशंसनीय प्रयास है।

मैं, इन पुस्तकों को तैयार करने में किए गए श्रमसाध्य प्रयासों और महानिदेशक, बीपीआरएंडडी तथा उनकी टीम द्वारा दिए गए निरंतर समर्थन की सराहना करता हूँ। मुझे विश्वास है कि ये पुस्तकें प्रभावी तरीके से साइबर अपराध का मुकाबला करने के लिए जांच अधिकारियों और कानून प्रवर्तन एजेंसियों का मार्गदर्शन करने में एक लम्बा सफर तय करेंगी।

(अमित शाह)

**कार्यालय : गृह मंत्रालय, नॉर्थ ब्लाक, नई दिल्ली-110001**
**दूरभाष :** 23092462, 23094686, **फैक्स : 23094221**
**ई-मेल :** hm@nic.in

अजय भल्ला, भा.प्र.से.
AJAY BHALLA, IAS

सत्यमेव जयते

गृह मंत्री
Home Secretary
भारत सरकार
Government of India
नॉर्थ ब्लॉक / North Block,
नई दिल्ली / New Delhi

# MESSAGE

Cyber criminals have already started misusing technology-controlled devices for perpetuating cyber-crimes which are posing huge challenges globally, affecting masses rather than individuals. It is very important to stay tuned with changing technology, new challenges, and threats in the field of cyber security and investigation, to ensure the cyber safety of our citizens. Widespread Phishing, Malware, Ransomware attacks, and other frauds pose a risk not just to individuals or platforms, but to our existence in many ways. The protection of critical services and infrastructure, fight against cyber crime, cyber incident response and recovery form a basis of cyber resilience strategy in the digital era.

2. National Cyber Crime Research & Innovation Centre, NCR&IC setup at BPR&D has been undertaking great efforts in this direction by undertaking research and development of innovative tools and software solutions to strengthen the Law Enforcement Agencies along with developing practical hands-on expertise based challenges like Capture The Evidence & Hackathons, Webinars, Conferences etc. They also work towards the capacity building of our LEAs through the relevant publication of books, proceedings of webinars and conferences and SOPs etc.

3. I appreciate DG, Mr. Balaji Srivastava and his team at BPR&D for the successful publication of these books and congratulate NCR&IC for this endeavour and hope these books will go a long way in guiding the investigating officers in effective cyber crime prevention and investigation.

9/6/22

**(Ajay Bhalla)**

Place : New Delhi
Dated : 09.06.2022

नित्यानन्द राय
NITYANAND RAI

गृह राज्य मंत्री
भारत सरकार
नार्थ ब्लाक, नई दिल्ली – 110001

MINISTER OF STATE FOR
HOME AFFAIRS
GOVERNMENT OF INDIA
NORTH BLOCK,
NEW DELHI - 110001

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

## संदेश

साइबर स्पेस में निरंतर तकनीकी प्रगति और हमारे जीवन में तीव्र गति से इसका सहज प्रसार, नई चुनौतियां, खतरे और कमजोरियां पैदा करता रहता है। सभी के लिए एक सुरक्षित साइबर अनुभव सुनिश्चित करने हेतु कड़े कदम उठाने की आवश्यकता है। भारतीय साइबर अपराध समन्वय केंद्र (I4C) के तहत बीपीआरएंडडी में स्थापित राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) क्षमता निर्माण और कानून प्रवर्तन एजेंसियों के प्रशिक्षण के लिए इस संबंध में विभिन्न पहल कर रहा है।

पुस्तकों का प्रकाशन, वेबिनार की कार्यवाही, सम्मेलन और एसओपी इस संबंध में राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) द्वारा की गई कई महत्वपूर्ण पहलों में से एक है। ये पुस्तिकाएं **"कानून प्रवर्तन की सेवा में एआई - एक परिचय", "महामारी के दौरान उभरते साइबर अपराध", "फर्स्ट रिस्पॉन्डर हैंडबुक- डुअल बूट सिस्टम और नेटवर्क ड्राइव", "क्लाउड इंफ्रास्ट्रक्चर से संबंधित साइबर अपराध", "गूगल डैशबोर्ड डेटा का अधिग्रहण और विश्लेषण"** राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) द्वारा प्रकाशित पुस्तकें निश्चित रूप से सुरक्षित साइबर अस्तित्व के अंतिम उद्देश्य को प्राप्त करने के लिए साइबर अपराध के खिलाफ इस लड़ाई में प्रभावी ढंग से अपनी भूमिका निभाने के लिए जांच अधिकारियों और कानून प्रवर्तन एजेंसियों को सक्षम करने में बहुत उपयोगी होगीं।

मैं इस महत्वपूर्ण प्रयास के लिए श्री बालाजी श्रीवास्तव, महानिदेशक, बीपीआरएंडडी और राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) को बधाई देता हूं और आशा करता हूं कि यह पुस्तक साइबर अपराध का पता लगाने, बढ़ते साइबर अपराधों की रोकथाम और जांच की दिशा में पेशेवर प्रतिक्रिया के नए आयाम जोड़ेगी।

**(नित्यानन्द राय)**

नई दिल्ली।

27 मई, 2022

Office Tel.: 011-23092870, 23092595, FAX No. : 011-23094896

**अजय कुमार मिश्रा**
**AJAY KUMAR MISHRA**

सत्यमेव जयते

गृह राज्य मंत्री
भारत सरकार
**MINISTER OF STATE FOR**
**HOME AFFAIRS**
**GOVERNEMNT OF INDIA**

## संदेश

वर्तमान समय में अपराधी इंटरनेट की गति, सुविधा और गुमनामी का फायदा उठाकर विभिन्न प्रकार की आपराधिक गतिविधियों को अंजाम दे रहे हैं। जैसे-जैसे प्रौद्योगिकी का विकास हो रहा है, वैसे-वैसे ही साइबर अपराधों की दर भी तेजी से बढ़ रही है। साइबर अपराधों के खतरों से प्रभावी ढंग से निपटने के लिए ज्ञान और कौशल को लगातार विकसित करते रहना अनिवार्य है, ताकि हमारी कानून प्रवर्तन एजेंसिया, साइबर अपराधियों से निपटने में हर प्रकार से सक्षम हों।

भारतीय साइबर अपराध समन्वय केंद्र (I4C) के तहत BPR&D में राष्ट्रीय साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC), MHA की स्थापना, कानून प्रवर्तन एजेंसियों की क्षमता निर्माण और प्रशिक्षण के लिए इस संबंध में विभिन्न पहल कर रहा है। साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) द्वारा **"AI में कानून प्रवर्तन की सेवा-एक परिचय", "महामारी के दौरान उभरते साइबर अपराध", "फर्स्ट रिस्पॉन्डर हैंडबुक-डुअल बूट सिस्टम और नेटवर्क ड्राइव", "क्लाउड इंफ्रास्ट्रक्चर से संबंधित साइबर अपराध", "Google डैशबोर्ड डेटा का अधिग्रहण और विश्लेषण"** नामक आगामी पुस्तिकाओं का प्रकाशन इस संबंध में एक सराहनीय प्रयास है।

मैं, इसके लिए महानिदेशक, बीपीआरएंडडी और उनकी सक्षम टीम के साथ-साथ साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC) के शोधकर्ताओं को बधाई देता हूँ और आशा करता हूँ कि ये पुस्तकें साइबर अपराधों से प्रभावी ढंग से निपटने में कानून प्रवर्तन अधिकारियों की मदद करने में काफी उपयोगी साबित होंगी

**(अजय कुमार मिश्रा)**

दिनांक: 01.06.2022
नई दिल्ली।

Office: Room No. 127, North Block, New Delhi-110 001 Tel.: 23094054 Fax: 23093549
E-mail: ajay.kumar19@sansad.nic.in

निशिथ प्रामाणिक
NISITH PRAMANIK

सत्यमेव जयते

गृह राज्य मंत्री
भारत सरकार
MINISTER OF STATE FOR
HOME AFFAIRS
GOVERNEMNT OF INDIA

## संदेश

साइबर अपराध की दुष्प्राप्य प्रकृति को देखते हुए कानून प्रवर्तन एजेंसियों के लिए आवश्यक है कि वह साइबर अपराधों को रोकने, अपराधों की पहचान और जाँच के लिए नई तकनीकों को अपनाएं। साइबर अपराध अनुसंधान और नवाचार केंद्र (NCR&IC), गृह मंत्रालय के भारतीय साइबर अपराध समन्वय केंद्र (I4C) के अंग के रूप में साइबर अपराधों की रोकथाम और जाँच के अपने प्रयासों में कानून प्रवर्तन एजेंसियों (LEAs) की क्षमता को मजबूत करने और बढ़ाने के लिए लगातार प्रयास कर रहा है।

इन पुस्तकों की तैयारी के साथ-साथ शोधित सॉफ्टवेयर टूल्स का विकास, वेबिनार, हैकाथॉन, सम्मेलन और प्रासंगिक पुस्तकों, कार्यवाही और मानक संचालन प्रक्रिया का प्रकाशन **"कानून प्रवर्तन की सेवा में एआई - एक परिचय", "महामारी के दौरान उभरते साइबर अपराध", "प्रथम प्रतिक्रियाकर्ता हैंडबुक - डयूल बूट सिस्टम और नेटवर्क ड्राइव्स", "Cloud Infrastructure से संबंधित साइबर अपराध", "Google Dashboard Data का अधिग्रहण और विश्लेषण"** इस दिशा में पुलिस अनुसंधान एवं विकास ब्यूरो और साइबर अपराध अनुसंधान और नवाचार केंद्र टीम के किए गए प्रयास वास्तव में महत्वपूर्ण हैं।

मुझे आशा है कि ये पुस्तकें साइबर अपराध की घटनाओं और इसकी जाँच से निपटने में बेहतर तैयारी के लिए देश भर के कानून प्रवर्तन अधिकारियों की सहायता करेंगी। इस दिशा में ब्यूरो के महानिदेशक, श्री बालाजी श्रीवास्तव एवं उनकी पूरी टीम के यह प्रयास निश्चित रूप से प्रशंसनीय है।

जय हिंद!

**(निशिथ प्रामाणिक)**

Office: Room No. 127-A, North Block, New Delhi-110 001 Tel.: 23092123 Fax: 23093143
E-mail : nisith.pramanik@sansad.nic.in

**बालाजी श्रीवास्तव,** भा.पु.से.
महानिदेशक

**Balaji Srivastava, IPS**
**Director General**

Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in

**पुलिस अनुसंधान एवम् विकास ब्यूरो**
**गृह मंत्रालय, भारत सरकार**
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

**Bureau of Police Research & Development**
**Ministry of Home Affairs, Govt. of India**
National Highway-8, Mahipalpur,
New Delhi-110037

## MESSAGE

The future of crime fighting is being defined by much of the same technology that is revolutionizing business and other areas of life. Artificial Intelligence (AI), automation, big data, extended reality, and all the most important trends we identify across other sectors are equally making their mark in policing. The COVID-19 Pandemic poses an unprecedented global challenge to all of society. Many have transferred their physical activities to online operations, as have criminals. Home-based working has increased the potential cybercrime victim pool. People take greater risks online at home which inadvertently exposes corporate IT to cybercriminals. Widespread Phishing, Malware, Ransomware attacks, and other frauds pose a risk not just to individuals or platforms, but to the masses in many different ways.

The National Cyber Research & Innovation Centre (NCR&IC) has been taking various initiatives in this regard in the form of research and development of innovative software solutions for LEAs, conducting webinars, conferences, and hackathons along with the publication of relevant booklets, proceedings, and SOPs.

It gives me great pleasure that the NCR&IC professionals have compiled five informative booklets on relevant topics which I am sanguine will be very informative as working manuals and ready reference for our LEAs.

The team of the Modernization Division of the BPR&D, led by Dr. Karuna Sagar, IPS, Director (Modernization), Brig. Navrattan Joshi (Retd), PSO (E), Dr. Manjunath Gosal, SSO (T), Dr. Sarabjit Kaur, Sh. Gourav Chaurasia, Sh. Farhan Sumbul, Sh. Amit Giri and Sh. Rushikesh Aghav truly deserves appreciation for the publication of these well-researched books.

I am confident that the NCR&IC, BPR&D will continue publishing such informative booklets, which will be very useful to LEAs in their fight against cybercrime and its effective investigation.

**(Balaji Srivastava)**

"Promoting Good Practices and Standards"

**डॉ. करूणा सागर,** भा.पु.से.
महानिरिक्षक / निदेशक (आधुनिकीकरण)

**Dr. Karuna Sagar, IPS**
**Inspector General/Director (Modernisation)**

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in



**पुलिस अनुसंधान एवम् विकास ब्यूरो**
**गृह मंत्रालय, भारत सरकार**
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

**Bureau of Police Research & Development**
**Ministry of Home Affairs, Govt. of India**
National Highway-8, Mahipalpur,
New Delhi-110037

## EXECUTIVE SUMMARY

Criminals have been exploiting the technological revolution to become more intense, technologically sophisticated, and potentially debilitating, posing serious threats and challenges. It is the need of this time to have consistent capacity up-gradation and proliferation of ushering technology to strengthen Law Enforcement agencies in ensuring that they always stay ahead of adversaries to proactively curb their initiatives so as to safeguard the security of citizens, critical processes and infrastructure of our Nation.

Publication of this booklet **"AI in the service of Law Enforcement - an Introduction"** is an endeavour in making our Law Enforcement Officers develop a better understanding of this technology, its types and the basic idea of the processes involved in making it operational right away from data to intelligence. This book describes various uses of this technology explored globally for the benefit of law enforcement exclusively. These use-cases are at different stages of development but have potential to benefit the law enforcement machinery in one way or the other in the coming span of time.

I hope this booklet will be a great guiding force for LEAs in understanding this ushering technology and its uses for the benefit of law enforcement so that a smooth sweep in adapting this technology and its effective manifestation can be undertaken for enhanced productivity and response.

I accord my heartiest congratulations to Dr Sarabjit Kaur, Cyber Crime Investigator/Researcher, NCR&IC for her tremendous efforts in the preparation of this booklet for the benefit of LEAs.

**(Karuna Sagar)**

"Promoting Good Practices and Standards"

# CONTENTS

# Acronyms

| | | |
|---|---|---|
| LEAs | : | Law Enforcement Agencies |
| AI | : | Artificial Intelligence |
| ML | : | Machine Learning |
| NLP | : | Natural Language Processing |

# 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) did not truly rise to prominence until last two decades, edging their way from the realms of science fiction and 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 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 advancements in software tools and solutions based on artificial intelligence for crime detection, prevention and investigation.

In the coming years, many more computer vision applications will be getting more sophisticated and making their way into the mainstream of police forces – with applications like predictive policing playing a significant role in ensuring better response and throughput.Gradual adoption will be attributed to a maturing AI ecosystem with more simple and intuitive user interface and overall enhanced user experience feedback.

## 1.1 Scope of use of Artificial Intelligence in context of Law Enforcement

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 utilization of 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 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 conceptualize 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. However, to avoid confusion, there is a merit in focusing, not on the technicality of AI and robotics and the complexity of the system, but rather on its functionality and usability. All that is required is to understand how it can enhance crime-fighting efforts and transform 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. Various applications of Artificial Intelligence are being developed to leverage the current crime handling paradigm but the states in which various foreseen applications or solutions lies can vary between being at the Conceptual / Research stage, Prototype stage, Under-Evaluation stage or Approved sage.

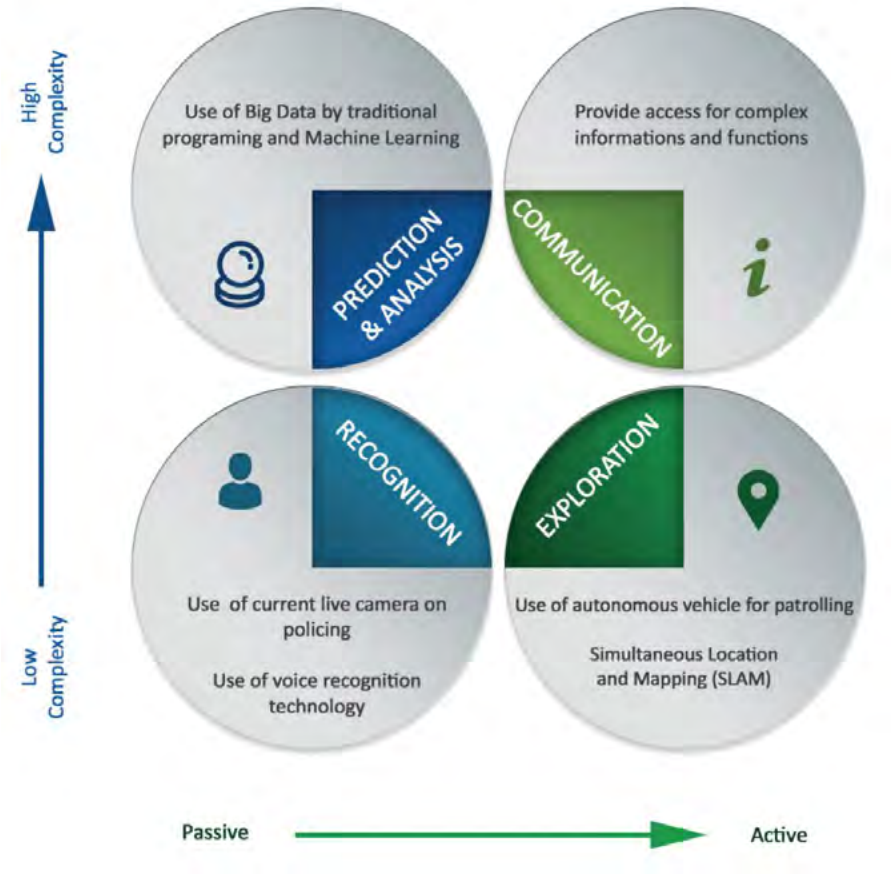



Figure1(file:///C:/Users/Administrator/Downloads/INTERPOLUNICRI%201st%20AI%20and%20Robotics%20Report%20(5).pdf)

## 1.2 Artificial Intelligence

AI is a rapidly advancing field of computer science. In the mid-1950s, John McCarthy, who has been credited as the father of AI, defined it as "the science and engineering of making intelligent machines". Conceptually, AI is the ability of a machine to perceive and respond to its environment independently and perform tasks that would typically require human intelligence and decisionmaking processes, but without direct human intervention.

AI is a technique that facilitates a machine to perform all cognitive functions such as perceiving, learning and reasoning that are otherwise performed by humans. "The Science and Engineering of making intelligent machines, especially intelligent Computer programs is Artificial intelligence" –John MC Carthy [Father of AI].

The yardstick to achieve true AI still seems decades away. Computers execute certain tasks way better than humans e.g.: Sorting, computing, memorizing, indexing, finding patterns etc. While

identifying emotions, recognizing faces, communication and conversation are unbeatable human skills. This is where AI will play a crucial role to enable machines in achieving equaling human capabilities.

**World Famous AI Machines (some instances):**

Google's AI-powered predictions (E.g.: Google Maps)

Ride-sharing applications (E.g.: Uber, Ola)

AI Autopilot in Commercial Flights

Spam filters on E-mails

Facial Recognition

Search recommendations on E-commerce and browsers

Voice-to-text features

Smart personal assistants (E.g.: Siri, Alexa)

Fraud protection and prevention.

Artificial Intelligence is a way of **making a computer, a computer-controlled robot, or a software that think intelligently,** in the similar manner as the intelligent humans do.

AI is accomplished by studying how human brain thinks, and how humans learn, decide, and work while trying to solve a problem, and then using the outcomes of this study as a basis of developing intelligent software and systems.

### 1.2.1 Philosophy of AI

While exploiting the power of the computer systems, the curiosity of human, lead him to wonder, "Can a machine think and behave like humans do?"

Thus, the development of AI started with the intention of creating similar intelligence in machines that we find and regard high in humans.

### 1.2.2 Goals of AI

- To Create Expert Systems – The systems which exhibit intelligent behavior,learn, demonstrate, explain, and advice its users.
- To Implement Human Intelligence in Machines – Creating systems thatunderstand, think, learn, and behave like humans.

## 1.3 AI - Technique

In the real world, the knowledge has some unwelcome properties –

- Its volume is huge, next to unimaginable.
- It is not well-organized or well-formatted.
- It keeps changing constantly.

AI Technique is a manner to organize and use the knowledge efficiently in such a way that –

- It should be perceivable by the people who provide it.
- It should be easily modifiable to correct errors.
- It should be useful in many situations though it is incomplete or inaccurate.

AI techniques elevate the speed of execution of the complex program it is equipped with.

### 1.3.1 AI system-variations

Building an AI system is a careful process of reverse-engineering human traits and capabilities in a machine, and using it's computational prowess to surpass what we are capable of.

To understand How Artificial Intelligence actually works, one needs to deep dive into the various sub domains of Artificial Intelligence and and understand how those domains could be applied into the various fields of the industry.

**Machine Learning:** ML teaches a machine how to make inferences and decisions based on past experience. It identifies patterns, analyses past data to infer the meaning of these data points to reach a possible conclusion without having to involve human experience. This automation to reach conclusions by evaluating data, saves a human time for businesses and helps them make a better decision.

**Deep Learning:** Deep Learning is an ML technique. It teaches a machine to process inputs through layers in order to classify, infer and predict the outcome.

**Neural Networks:** Neural Networks work on the similar principles as of Human Neural cells. They are a series of algorithms that captures the relationship between various underlying variables and processes the data as a human brain does.

**Natural Language Processing:** NLP is a science of reading, understanding, interpreting a language by a machine. Once a machine understands what the user intends to communicate, it responds accordingly.

**Computer Vision:** Computer vision algorithms tries to understand an image by breaking down an image and studying different parts of the objects. This helps the machine classify and learn from a set of images, to make a better output decision based on previous observations.

**Cognitive Computing:** Cognitive computing algorithms try to mimic a human brain by analyzing text/speech/images/objects in a manner that a human does and tries to give the desired output.

### 1.3.2 AI System - Basic Applications domain

**Machine Learning**

At the core of AI and the basis of many of the other examples. This technology makes it possible for a machine to learn and from past experiences and deliver output based on provided data, without being programmed to do so repeatedly. Example: Google calculating travel time based on live traffic data

**Deep Learning**

Deep learning is a more complicated version of machine learning, stacking multiple layers of algorithms between the input and output layer. This makes it possible for deeplearning to make intelligent decisions based on several hierarchical concepts. Example: Personalized Netflix recommendations

**Speech Recognition**

Speech processing or recognition allows a machine to recognize and interpret human speech. This technique makes it possible to translate words to text, similar to a transcriber. It can also translate simple commands from humans to actions understood and performed by machines. Example: Apple's Siri calling a contact by voice demand

**Natural Language Processing**

Natural language processing is a more sophisticated type of speech recognition. By using deep learning technology, it has the ability to determine the intent of the spoken words. This unlocks the possibility to have dialogues with machines hard to distinguish as artificial. Example: Personalized autocomplete function in WhatsApp

**Image processing**

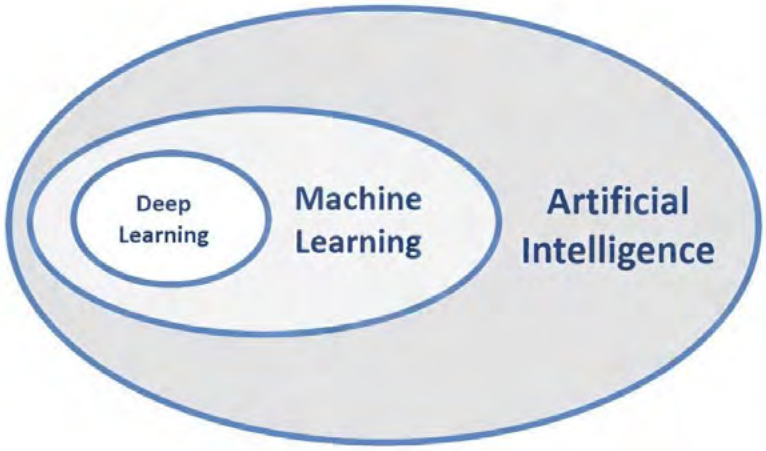
Image processing is using algorithms to enhancing, restore, compress or analyze an image, allowing to extract more information from an image. Example: Google translating text directly with your phone's camera

**Computer vision**

Computer vision 'understands' the meaning of an image. This allows machines to process images and recognize the information presented by its visual features.

Example: Facebook detecting and censoring prohibited pictures

**Relationship between AI, ML, and DL?**




As the above image portrays, the three concentric ovals describe DL as a subset of ML, which is also another subset of AI. Therefore, AI is the all-encompassing concept that initially erupted. It was then followed by ML that thrived later, and lastly DL that is now promising to escalate the advances of AI to another level.

## 1.4 Types of Artificial Intelligence

Different Artificial Intelligence entities are built for different purposes, and that's how they vary.

### 1.4.1 Three Broad Types of Artificial Intelligence

AI technologies are categorized by their capacity to mimic human characteristics, the technology they use to do this, their real-world applications etc.Using these characteristics for reference, all artificial intelligence systems - real and hypothetical - fall into one of three types:

Artificial Narrow Intelligence (ANI): It is about Machine Learning.It specializes in one area and solves one problem. For ex Siri, Alexa etc.

Artificial General Intelligence (AGI): It is about Machine Intelligence. It refers to a computer that is as smart as a human across the board.

Artificial Super Intelligence (ASI): It is about Machine Consciousness. It imbibes intellect that is much smarter than the best human brains in practically every field or aspect.

### 1.4.2 Strong and Weak Artificial Intelligence

Extensive research in Artificial Intelligence also divides it into two more categories, namely Strong Artificial Intelligence and Weak Artificial Intelligence. The terms were coined by John Searle in order to differentiate the performance levels in different kinds of AI machines. Here are some of the core differences between them.

| Weak AI | Strong AI |
|---|---|
| It is a narrow application with a limited scope. | It is a wider application with a vaster scope. |
| This application is good at specific tasks. | This application has an incredible human-level intelligence. |
| It uses supervised and unsupervised learning to process data. | It uses clustering and association to process data. |
| Example: Siri, Alexa. | Example: Advanced Robotics |

## 1.5 Purpose of Artificial Intelligence

The purpose of Artificial Intelligence is to aid human capabilities and help us make advanced decisions with far-reaching consequences. That's the answer from a technical standpoint. From a philosophical perspective, Artificial Intelligence has the potential to help humans live more meaningful lives devoid of unnecessary hard labour, and help manage the complex web of interconnected individuals, companies, states and nations to function in a manner that's beneficial to all of humanity.

That's all in the far future though – we're still a long way from those kinds of outcomes. Currently, Artificial Intelligence is being used mostly by companies to improve their process efficiencies, automate resource-heavy tasks, and to make business predictions based on hard data rather than gut feelings.

AI is used in different domains to give insights into user behavior and give recommendations based on the data. For example, Google's predictive search algorithm used past user data to predict what a user would type next in the search bar. Netflix uses past user data to recommend what movie a user might want to see next, making the user hooked onto the platform and increase watch time. Facebook uses past data of the users to automatically give suggestions to tag one's friends, based on their facial features in their images. AI is used everywhere by large organizations to make an end user's life simpler. For instance:

- Searching within data, and optimizing the search to give the most relevant results.

- Logic-chains for if-then reasoning, that can be applied to execute a string of commands based on parameters.
- Pattern-detection to identify significant patterns in large data set for unique insights.
- Applied probabilistic models for predicting future outcomes.

## 1.6 Advantages of Artificial Intelligence

There's no doubt in the fact that technology has made our life better. From music recommendations, map directions, mobile banking to fraud prevention, AI and other technologies have taken over a lot more.Let us take a look at some advantages of Artificial Intelligence-

Advantages of Artificial Intelligence (AI)

Reduction in human error

Available 24×7

Helps in repetitive work

Digital assistance

Faster decisions

Rational Decision Maker

Medical applications

Improves Security

Efficient Communication

# 2. How Machine Learning Works - Broad overview

Machine learning is a data analytic technique that teaches computers to do what comes naturally to humans and animals: learn from experience. Machine learning algorithms use computational methods to "learn" information directly from data without relying on a predetermined equation as a model. The algorithms adapt and improve their performance as the number of samples available for learning increases.

With the rise in big data, machine learning has become a key technique for solving problems. Consider using machine learning when you have a complex task or problem involving a large amount of data and lots of variables, but no existing formula or equation. For example, machine learning is a good option if you need to handle situations like these:

Hand-written rules and equations are too complex—as in face recognition and speech recognition.

The rules of a task are constantly changing—as in fraud detection from transaction records.

The nature of the data keeps changing, and the program needs to adapt—as in automated trading, energy demand forecasting, and predicting shopping trends etc.

## 2.1 Machine learning - Basic Techniques

Machine learning uses two types of techniques: supervised learning, which trains a model on known input and output data so that it can predict future outputs, and unsupervised learning, which finds hidden patterns or intrinsic structures in input data.

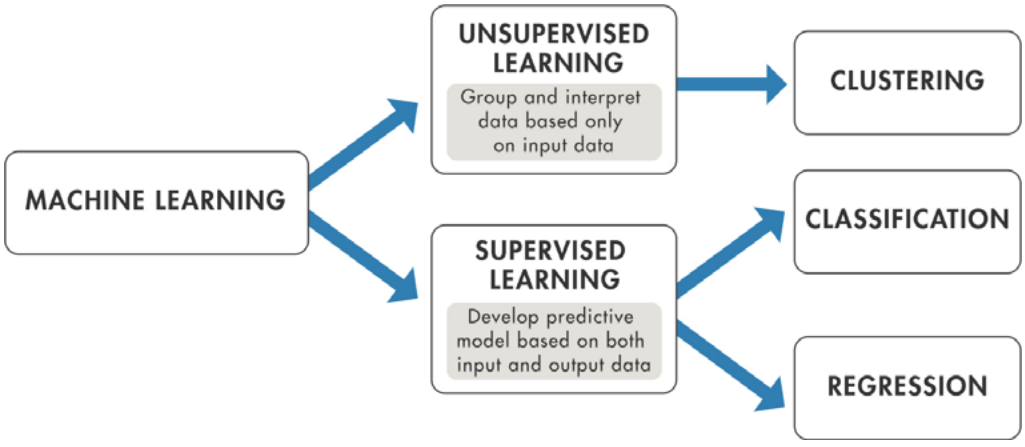



Figure 2 : Machine learning techniques include both unsupervised and supervised learning.

## Supervised Learning

Supervised machine learning builds a model that makes predictions based on evidence in the presence of uncertainty. A supervised learning algorithm takes a known set of input data and known responses to the data (output) and trains a model to generate reasonable predictions for the response to new data. Use supervised learning if you have known data for the output you are trying to predict.

Supervised learning uses classification and regression techniques to develop machine learning models.

Classification techniques predict discrete responses—for example, whether an email is genuine or spam, or whether a tumor is cancerous or benign. Classification models classify input data into categories. Typical applications include medical imaging, speech recognition, and credit scoring.

Use classification if your data can be tagged, categorized, or separated into specific groups or classes. For example, applications for hand-writing recognition use classification to recognize letters and numbers. In image processing and computer vision, unsupervised pattern recognition techniques are used for object detection and image segmentation.

Regression techniques predict continuous responses—for example, changes in temperature or fluctuations in power demand. Typical applications include electricity load forecasting and algorithmic trading.

Use regression techniques if you are working with a data range or if the nature of your response is a real number, such as temperature or the time until failure for a piece of equipment.

## Unsupervised Learning

Unsupervised learning finds hidden patterns or intrinsic structures in data. It is used to draw inferences from datasets consisting of input data without labeled responses.

Clustering is the most common unsupervised learning technique. It is used for exploratory data analysis to find hidden patterns or groupings in data. Applications for cluster analysis include gene sequence analysis, market research, and object recognition.

For example, if a cell phone company wants optimize the locations where they build cell phone towers, they can use machine learning to estimate the number of clusters of people relying on their towers. A phone can only talk to one tower at a time, so the team uses clustering algorithms to design the best placement of cell towers to optimize signal reception for groups, or clusters, of their customers.

**Reinforcement Learning :** The reinforcement learning is totally different from both supervised and unsupervised ML. The relationship among supervised and unsupervised learning can be related with each other with the presence and absence of labels. However, the reinforcement learning learns

from the mistakes. Reinforcement learning (RL) is an area of machine learning concerned with how intelligent agents ought to take actions in an environment in order to maximize the notion of cumulative reward. The signals to the algorithms are provided that can associate the good behaviour with positive signals and bad behaviour with negative label. The algorithms can reinforce algorithms to prefer good behaviour and bad behaviors. With the passage of time, the algorithm can learn to make fewer mistakes as it was initially

## 2.2 Choosing the adequate Machine Learning Algorithm

Choosing the right algorithm can seem overwhelming—there are dozens of supervised and unsupervised machine learning algorithms, and each takes a different approach to learning.

There is no best method or one size fits all. Finding the right algorithm is partly just trial and error—even highly experienced data scientists can't tell whether an algorithm will work without trying it out. But algorithm selection also depends on the size and type of data you're working with.

Choose supervised learning if need is to train a model to make a prediction—for example, the future value of a continuous variable, such as temperature or a stock price, or a classification—for example, identify makes of cars from webcam video footage.

Choose unsupervised learning if need is to explore your data and want to train a model to find a good internal representation, such as splitting data up into clusters.

## 2.3 Training, validating, and testing data for machine learning

Machine learning is a process, just as everything is a process in the world of computers. To build a successful machine learning solution, you perform these tasks as needed, and as often as needed:

**Training:** Machine learning begins when you train a model using a particular algorithm against specific data. The training data is separate from any other data, but it must also be representative. If the training data doesn't truly represent the problem domain, the resulting model can't provide useful results. During the training process, you see how the model responds to the training data and make changes, as needed, to the algorithms you use and the manner in which you massage the data prior to input to the algorithm.

**Validating:** Many datasets are large enough to split into a training part and a testing part. You first train the model using the training data, and then you validate it using the testing data. Of course, the testing data must again represent the problem domain accurately. It must also be statistically compatible with the training data. Otherwise, you won't see results that reflect how the model will actually work.

**Testing:** After a model is trained and validated, you still need to test it using real-world data. This step is important because you need to verify that the model will actually work on a larger dataset that you haven't used for either training or testing. As with the training and validation steps, any data you use during this step must reflect the problem domain you want to interact with using the machine learning model.

**Training** provides a machine learning algorithm with all sorts of examples of the desired inputs and outputs expected from those inputs. The machine learning algorithm then uses this input to create a math function. In other words, training is the process whereby the algorithm works out how to tailor a function to the data.

To give an idea of what happens in the training process, imagine a child learning to distinguish trees from objects, animals, and people. Before the child can do so in an independent fashion, a teacher presents the child with a certain number of tree images, complete with all the facts that make a tree distinguishable from other objects of the world. Such facts could be features, such as the tree's material (wood), its parts (trunk, branches, leaves or needles, roots), and location (planted in the soil). The child builds an understanding of what a tree looks like by contrasting the display of tree features with the images of other, different examples, such as pieces of furniture that are made of wood, but do not share other characteristics with a tree.

A machine learning classifier works the same. A classifier algorithm provides a class as an output. For instance, it can reveal that the photo provided as an input matches the tree class (and not an animal or a person). To do so, it builds its cognitive capabilities by creating some mathematical formulation that includes all the given input features in a way that creates a function that can distinguish one class from another.

# 3. Artificial Intelligence for Law Enforcement

Many applications of Artificial intelligence and machine learning are being formulated and explored for the law enforcement but their availability depends upon weather the solutions are completely developed or are being researched i.e. are under Analysis, improvisation or development phase and some are just getting explored.

## 3.1 AI Based Facial Recognition

Computerized facial recognition is a relatively new technology, being introduced by law enforcement agencies around the world in order to identify persons of interest. Coupled with an automated biometric software application, this system is capable of identifying or verifying a person by comparing and analyzing patterns, shapes and proportions of their facial features and contours.

Intelligent, AI-based facial recognition technology is software that can instantaneously search databases of faces and compare them to one or multiple faces that are detected in a scene.

### 3.1.1 AI FACIAL RECOGNITION-Basics

Each person's face is broken up into numerous data-points; these can be the distance between the eyes, the height of the cheekbones, the distance between the eyes and the mouth, and more advanced features which can be taken into consideration now due to use of artificial intelligence like neural textures, expressions I.e dynamic characteristics along-with static characteristics to recognize faces. on. AI facial recognition searches on those data-points and tries to account for variations and identification. AI facial recognition searches on those data points and tries to account for variations (for instance, distance from the camera and slight variations in the angle of the face). Face recognition recognizes a human face without any physical contact required. The solution runs through algorithms that match the facial nodes/data points of a person to the images saved in the database.The police authorities are alerted if the system shows a face match.

### 3.1.2 Advanced facial recognition systems with Artificial Intelligence

Advanced facial recognition systems using artificial intelligence are handling criminal database creation task also intelligently,when an image or face needs to be stored into the database its various images projecting different angular poses and variations like dim image, partial image and image changes due to ageing etc. are assessed and created and stored using AI software so that comparison of input to such a database can be made more efficiently and speedily.

These days as AI has enabled facial recognition to work on facial expressions and neural textures also thus performing behaviour analysis or identification of anomalous / suspicious behaviour has also

become possible.

### 3.1.3 Video & Image Processing

Video processing is a technique of achieving intelligence in the computer vision field. Like humans computers have eyes to, through cameras though, but they lack the ability to understand the world as we humans do. With video image processing we can bridge the gap. How it is achieved is by considering video frames as images and process those images using image processing techniques where we can see video processing as a collection of image processing tasks. For example, the background can be subtracted from the foreground by considering a sequence of N video frames as images and by taking the statistical average of the continuous image sequence. Video processing is not one task, but a result of a collection of sub tasks.

In video processing, a video will be read frame by frame, and for each frame, image processing will be applied to extract the features from that frame. To extract features, many filters have to be applied to the image. All these tasks are performed as mathematical functions. Face Recognition system works in multiple steps. First the faces are identified in the frame by using a pee-trained model trained on thousands of images. After face detection pose estimation on each image is done to make sure we get a good frontal face. After making sure we are getting a good view of the front face the key points on the faces are identified. These points are eyes, nose, lips and jaw line. These points help us to identify a person. For each person identified in the frame we compare each person's facial points with points of the individuals in the database. Since these points are decimals thousands of comparisons can be done in a matter of milliseconds.

**3.1.4 Object Detection :** Like face detection AI models are even being trained to detect objects like bags and weapons. Since the model has been trained on different types of images so the shape, color, size and type of the object does not matter as long as the model has been trained to identify it.

### 3.1.5 Centralized Monitoring System fed by CCTV's

Centralized Monitoring System fed by CCTVs across the city in places including Schools / Colleges, Parks, Malls ,Major markets and crossings etc.is fed into Video and Image Analytic to generate real time alerts with special focus on chain snatching, women harassment and loot using along with it Data Analytic and Integrating emergency number data and inputs to focus more on camera feeds to identify criminals and to respond in fastest possible way.

Such system can be used to identify people and objects in images, prerecorded videos and live videos. Such systems of facial recognition and video processing can be connected with the live feed of the camera and such camera footage/physical location of entities can be identified through the IP of the camera.During live feed, the object and character (Human) matching begins. The software is constantly comparing the feed with the trained models (Criminals, missing children, Guns, bags, sticks

etc.). Every match is stored and on a predefined protocol, the alerts can be customized.

### 3.1.6 Outcomes of AI Enabled Facial Recognition systems:

- ✓ Identification and Tracking of criminals
- ✓ Detecting suspicious behaviour and preventing crimes and also in finding potential suspects of the crime.
- ✓ Detecting and preventing Violence
- ✓ Unclaimed objects
- ✓ Find missing children / person
- ✓ Prevent illegitimate intrusion or trespassing
- ✓ Search lost or stolen cars/vehicles
- ✓ Identification of Dead-bodies.

## 3.2 Surveillance and Face recognition

Surveillance technologies have evolved beyond the security camera in a mall or airport like

- ✓ CCTV CAMERAS with AI CHIPS:

Real time or proactive monitoring and surveillance and alerts for crime detection and prevention has added to the usual capacity of application of normal CCTV cameras.

- ✓ Unmanned DRONES
- ✓ Patrol drones
- ✓ Communication robots with mobile camera.

### 3.2.1 CCTV CAMERAS with AI CHIPS:

Real time or proactive monitoring and surveillance and alerts for crime detection and prevention has added to the applicability of normal CCTV cameras.These can be used for following applications:

- ✓ Identification and Tracking of criminals
- ✓ Detecting suspicious behaviour and preventing crimes and also in finding potential suspects of the crime.
- ✓ Detecting and preventing Violence
- ✓ Unclaimed objects

- ✓ Find missing children / person
- ✓ Prevent illegitimate intrusion or trespassing
- ✓ Search lost or stolen cars/vehicles
- ✓ Identification of Dead-bodies.

### 3.2.2 Unmanned DRONES with AI capacity


FIGURE 3(SOURCE https://www.dronevolt.com/en/engineering-consulting/artificial-intelligence-applications-for-uav/)

Artificial intelligence gives machines the ability to interact in an intelligent way. This is why the fusion between drones and artificial intelligence represents the response to many needs in aerial imagery and provides new headlines in the future of aerial technology using computer vision and neural networks.

### Drones with AI can evolve to various applications.

- Object detection, counting, segmentation and tracking
- Person or animal detection and tracking
- Crowd counting
- Thermal detection
- Check compliance of the use of face masks in public spaces and in professional places
- Detection of the use of protective equipment (glasses and helmets)
- Face detection and recognition
- Fire and smoke detection

- License plate reading
- Crack damage detection on surfaces
- Patrol drones
- Communication robots with mobile camera.

### 3.2.3 Robotic birds

Birds are everywhere, and most people do not give them much attention. This fact has brought about an interest in using bird forms to carry out surveillance.

Robotic birds capable of autonomy and staying in the air for more than a few minutes. Many sophisticated bird robots are evolving depending upon the functionality they are required to deliver.

### 3.2.4 Smart glasses

Another way the surveillance might be monitoring its citizens is through "smart" glasses equipped with facial recognition software to scan faces and match them to persons of interest in seconds. These augmented reality (AR) eyewear provide law enforcement with a quick way to patrol a large number of people

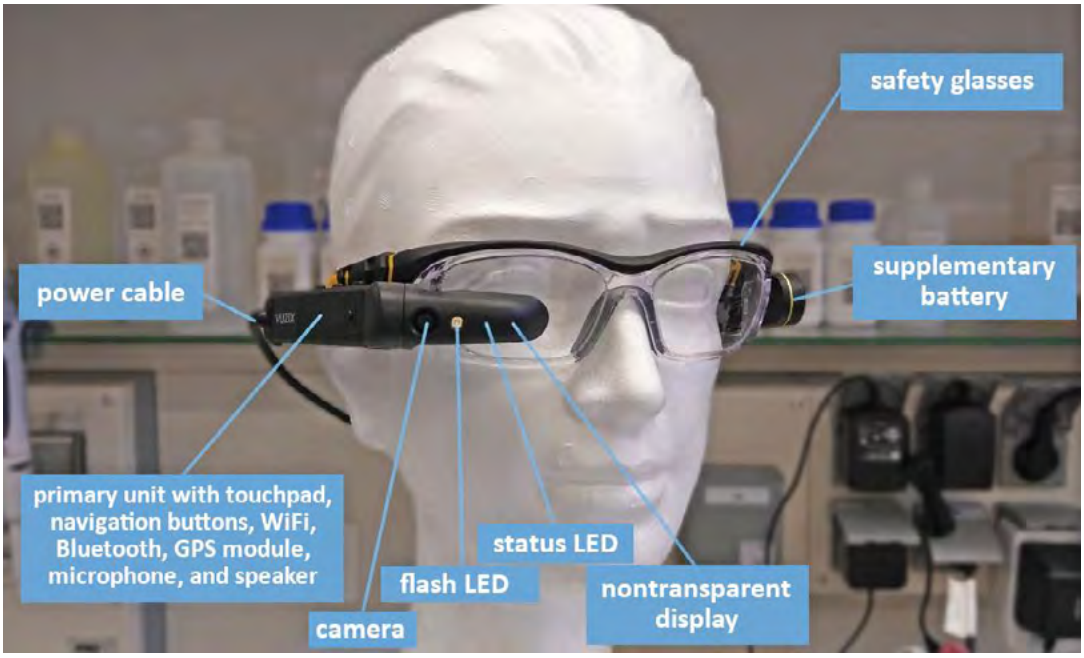



Figure4 (https://www.chemistryviews.org/details/ezine/11298556/Smart_Glasses_Tool_or_Toy__Part_1.html)

This lightweight eyewear device contains a front-facing camera, motion tracker, and a display on each lens.

### 3.2.5 Body worn Cameras

Body-worn cameras would help the Department assess the quality of response by the police personnel in an emergency situation.

Figure 5

The cameras could also be used to shoot visuals at night. Visuals of important events, as in the case of a conflict, would be saved at the computer of the respective police station for future references.

It provides mobile surveillance with artificial intelligence ability to not only record but identify criminals and missing people from the crowd or identify stolen vehicles automatically and can alarm for wanted criminals/vehicles/missing children, wherever identified so that in real time action can be taken.

### 3.2.6 Use of AI for Surveillance and Face recognition

- CCTV CAMERAS with AI CHIPS
- DRONES
- Body worn Cameras

✓ Identification and Tracking of criminals

✓ Detect suspicious behaviour,violence,unclaimed objects

✓ Find missing children/person

✓ Prevent illegitimate intrusion or trespassing

✓ Search lost or stolen cars/vehicles

✓ Identification of Dead-bodies.

## 3.3 Application of AI based Technologies for Automation in Cyber Crime Investigation , Forensic Science and Data Analysis

Artificial intelligence has been used for the following applications in the field of Analysis and Investigation:

- Facial recognition systems : Facial recognition systems have become sophisticated with the use of AI to identify/recognize the person with enhanced accuracy and are even striving to tap the dim, masked or partial inputs.
- Face Validation software : Face Validation software is also also being developed, using AI to detect when a person is not who they seem.
- **Biometric matching tools :** Biometric matching tools from old or unclear samples.

Pattern recognition is a process of automatic machine recognition, which is categorized according to the type of learning procedure used to generate the output value. Identification and comparison of specific types of patterns in the suspected data is one of the crucial elements of forensic science. The experts have to analyse a huge amount of data with heavy statistical and probabilistic reasoning techniques. A pattern could be anything like a fingerprint image, a handwritten cursive word, a human face, or a speech signal. Neural networks along with its advancements like CNN,RNN etc have been used in many areas such as interpreting visual scenes, speech recognition, face recognition, fingerprint recognition, iris recognition etc.

Deep learning has made tremendous success in the field of computer vision and pattern recognition as it does not require handcrafted feature extraction. Deep learning automatically learns features and structures under a sufficient number of input training data. These advantages of artificial intelligence make it suitable for various tasks in automatic fingerprint identification and classification systems. Also these automated AI based systems can substantially bring down the number of comparisons at the time of matching with high accuracy .

- **DNA Matching :** Pattern recognition ability of artificial intelligence augmented with deep learning methods has potential to yield DNA Matching in hrs.not days.
- **Crime intelligence and criminal data Analysis tool**-using social media and open source etc.

  AI-powered open-source intelligence tools (including open-source intelligence tools for social media) accelerate open-source investigations through the power of AI. For example, collecting vast amounts of OSINT data isn't enough, the data must also be analyzed for connecting the dots. When done manually, this painstaking process requires significant

investments vis-a-vis time and people; with the risk that valuable insights may be missed. An AI-driven platform surely can aid in increased productivity and quicker conclusions.

AI driven software can be augmented with multi-modal criminal data (i.e text, images, audio or video) to be analyzed for criminal leads on the basis of multi-modal input parameters at a much faster pace and in an automatic manner to enhance effective response.

- **Tool to identify PROXY /VPN enabled system along with source IP.**

  Concealing a person's true identity and location on the Internet can be done by the usage of proxy or anonymity services. Cyber criminals commit fraudulent transactions by using proxy services to hide their real internet protocol (IP) address and physical location, in order to avoid being tracked and prosecuted by law enforcement agencies. Thus, having the ability to detect proxy connections and prevent fraudulent transactions becomes paramount. A solution to detect usage of anonymising proxies is being developed using a Multi-layered neural network that is trained using data found in the Transmission Control Protocol (TCP) header of captured network packets etc. and many researchers are manifesting the strength of artificial intelligence in exploring solution of this problem too.

- **AI tool for 3D crime scene mapping,Crime related data and evidence corelation to yield investigation intelligence and listing of objects using that.**

  The applications of 3D digital technologies and artificial intelligence (AI) could be used to enhance phases of forensic visualization. It can create 3D graphical models and animations automatically to provide real-time interactivity of the reconstructed scenes. Virtual reality simulation in the forensic process involves graphical modeling of 3D virtual objects and humans based on measurements and photos and animates the models to recreate the crime scene or incidents concerned. These field of forensic animation include pathological visualization, murder reconstruction, and shooting case evaluation etc.

- **Data analysis and extraction of intelligence from seized devices.**

  The use of Artificial Intelligence in computer forensics composed of specialized intelligent expert systems that act based on the experts knowledge of the technical domain.

  Their goal is to analyze and correlate the data contained in the evidences of an investigation and based on its expertise, present the most interesting evidence to the human examiner, thus reducing the amount of data to be personally analyzed. The correlation feature helps to find links between evidences that can be easily overlooked by a human expert, specially due to the amount of data involved.Similarly for other domains too software solutions are being developed using artificial intelligence.

- **Detection of Deep-fakes, morphed or doctored contents using deep learning and advanced neural networks.** Deepfake techniques, which present realistic AIgenerated videos of people doing and saying fictional things, have the potential to have a significant impact on how people determine the legitimacy of information presented online. These content generation and modification technologies may affect the quality of public discourse and the safeguarding of human rights — especially given that deepfakes may be used maliciously as a source of misinformation, manipulation, harassment, and persuasion. Identifying manipulated media is a technically demanding and rapidly evolving challenge that requires collaborations across the entire tech industry and beyond for research and development of software solutions to detect such content. AI is being manifested to develop solutions to detect deepfake in multi-modal inputs.

- **Forensic tools for Memory forensics , Mobile forensics, Cloud forensics and much more in the field of Forensics and Investigation.**

  AI provides the capacity to overcome human errors during image, video or CCTV footage analysis during criminal investigation. Traditional software algorithms that assist human experts are limited to predetermined features like eye shape, eye color, distance between eyes for facial recognition and demographics information for pattern analysis. The AI algorithms developed for multimedia analysis could not only learn complex tasks but also can develop and determine their own independent complex facial recognition features & parameters to accomplish given tasks. These advanced AI algorithms have the potential to match faces, identify weapons, compare voices and detect complex events such as accidents or crimes . Various AI based algorithms have been aiding security personnel and experts for audio analysis and speaker identification. Artificial intelligence in speech recognition is also used for speech fluency evaluation and language instruction .

  **Digital forensics.** Digital forensics is a highly developing science which is becoming increasingly important in computation and requires the intelligent analysis of huge amounts of very complex data sets. A large number of potentially related evidences are more vulnerable to disturb or diminish during the forensic examinations. This problem is not only related to forensic computing, but also to network incident response. So AI is an ideal approach to deal with many of the such complex problems that currently exist in it.

  Currently used conventional and manual approaches for searching and examining the data are not sufficient to deal with the size of the problem currently found in digital forensics. The aim of intelligent and autonomous agents that compose the AI powered system is to analyze and correlate the data contained in the evidences of an investigation and based on its expertise, present the most interesting evidence to the human examiner. Thus these

systems eventually reduce the amount of data to be personally analyzed and give a subset that is more likely an important and desirable evidence to the investigation.

**Network forensics** is the branch of digital forensic, which involves the study of analyzing network activity in order to discover the source of security policy violations or information assurance breaches. Forensic analysis by capturing network activity is trivial in practice and all the information captured or recorded will not be necessary to be useful for analysis. Application of artificial intelligent tools and techniques can overcome these challenges by offline intrusion analysis, and protecting the integrity and confidentiality of the information infrastructure. These AI powered tools are essential for ensuring information assurance by updating the newly identified security breaches into the protection and detection mechanisms of organizations.

- **Application to convert vernacular language context to English from multimodal inputs to reduce human intervention in translating significant documents.**
- **Analysis of Financial data to handle suspicious patterns to detect Frauds etc.**

  Artificial Intelligence has therefore emerged as a significant tool for avoiding financial crimes due to its increased efficiency. AI can be used to analyze huge numbers of transactions in order to uncover fraud trends, which can subsequently be used to detect frauds.

- **Tracking of organized crime / criminal gangs**

  Artificial intelligence and pattern recognition along with its well trained models are being explored to bring-forth the organized crime/ criminal gangs in a physical location.

  Estimation of range of a projectile will be much easier when AI will be contributing the ballistics field. Artificial Neural Network can guide experts for searching gunpowder, cartridge case and help them for comparison of bullet marks, firearm identification and other ballistic evidence from the database itself with the help of image processing without any manual interference.

## 3.4 Predictive Policing or Crime Prediction

The rise of AI technologies are aiding the police and security professionals for not only crime detection, but also crime prevention and prediction. Some of the advanced algorithms of AI are developed to detect crime patterns and suspicious anomalies, predict future crime spots, assess criminal risk factors, and to uncover criminal networks .Various machine-learning and artificial intelligence based algorithms are used to predict the future crime spots by analyzing the spread of crime types, crime location, and criminal weapons . Briefly, an AI powered system can successfully

aid for the prediction of crime spots using the process of AI,deep learning and data mining and to predict tendency of a person to commit a crime, in future using facial recognition and tracking one's behavioral changes.

**Predictive Policing can lead to**

- Enhanced Accuracy and granularity
  - Hot-spot Prediction
  - Crime forecasting
  - Efficient manpower Management.
  - Better security ensured for high crime risk area

## 3.5 Use Cases of AI for CYBER SPHERE

- **Tools for monitoring of social media- proactive monitoring.**

  Social media has become a repository of information, opinions, relationships, ideologies with imbibed sentiments. This makes Social Media a salient platform for monitoring and analysis of individuals, groups, and events - proactively. This information, rather data is of crucial importance to the law enforcement agencies for tracking and monitoring of suspects, criminals and their movements.

- **Tool for Sentiment analysis and hate speech analysis to predict and handle - movements which can challenge peace/security/law & order.**

- **Fake news detection and mitigation using Artificial Intelligence algorithms.**

  Social media due to its low cost, easy access, and rapid dissemination of information lead people to seek out and consume news from social media at the same time social media enables the wide spread of "fake news" too, i.e., low quality news with intentionally false information. The extensive spread of fake news has the potential for extremely negative impacts on individuals and society. Therefore, fake news detection on social media has recently become an emerging research that is attracting tremendous attention of artificial intelligence community.Fake news detection and mitigation using Artificial Intelligence algorithms is being evolved using its various approaches to train the models in distinguishing between peace of information/news as real or fake.

- **Fake profile identification.**

  At present social network sites are part of the life for most of the people. Every day several people are creating their profiles on the social network platforms and they are interacting

with others independent of the user's location and time. The social network sites not only providing advantages to the users and also provide security issues to the users as well their information. To analyze, who are encouraging threats in social network we need to classify the social networks profiles of the users. From the classification, we can get the genuine profiles and fake profiles on the social networks. Traditionally, different classification methods for detecting the fake profiles on the social networks were used. To improve the accuracy rate of the fake profile detection in the social networks Machine learning and Natural language Processing (NLP) techniques are being used to improve the accuracy rate of the fake profiles detection.

1) The detection process starts with the selection of the profile that needs to be tested.
2) After the selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.
3) The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier.
4) The classifier determines whether the profile is fake or genuine.
5) The classifier may not be 100% accurate in classifying the profile so; the feedback of the result is given back to the classifier.
6) This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles

- **Identification of phishing links and alerts**

In phishing and its common variants, the attackers create website pages by copying genuine websites and send suspicious URLs to the targeted victims through spam messages, texts, or online social networking. An attacker scatters a fake variant of an original website, through email, phone, or content messages, with the expectation that the targeted victims would accept the cases in the email made. They will likely target the victim to include their personal or highly sensitive data. AI-enabled phishing attacks detection techniques using AI and deep learning methodology is being researched and evolved.

- **Deep and dark web monitoring tool.**

Beneath the surface web, the public form of the internet exists a concealed "dark web." Host to anonymous, password-protected sites, the dark web is where criminal marketplaces thrive in the illegitimate advertising and selling. Law enforcement agencies work continuously to stop these activities, but the challenges faced in investigating and prosecuting the real-world people behind the users who post on these sites are tremendous.

To overcome this challenge, researchers are developing new software tools using machine learning to analyze deep and dark-web data.

- **Prevention & mitigation of spread of obscene content on online platforms using Artificial intelligence based software solutions.**
- **Suspicious visitors tracking on financial web-apps/sites using pattern matching and deep learning.**
- **Social media analytic for Women and child safety-cyberbully detection and mitigation tool.**
- **AI enabled Chat-bots for crime prevention , awareness & guidance and counselling of victims.**

## 3.6 Use of AI For Traffic Management

Use of Artificial intelligence is being explored for the following:

- Traffic control & Management
- Prediction of hot spots
- Automatic number plate recognition & Handling of fine/challans

## 3.7 Surveillance of Prison and Borders

**Surveillance of prison and borders using artificial intelligence enabled**

- DRONES
- AI Cameras

has enabled:

- ✓ Aerial surveillance of jail and borders.
- ✓ Identification of Suspicious behaviour and objects in the localized proximity
- ✓ 3d mapping for planning operations and training
- ✓ Predict recidivism of criminals/ juvenile at prisons
- ✓ Drones are ideal first responders. Drones are faster than conventional vehicles when used as first responders. They can reach a location within minutes after receiving an emergency request, and aerially assess the situation before human responders arrive.
- ✓ Drones for disaster management specially at remote border areas.

# Conclusion

Artificial intelligence has greatly impacted the shape of various use-cases or applications for law enforcement and has increased the accuracy,efficiency and effectiveness of many but its yet to achieve its full strength as it is evolving over the period of time and many software solutions are yet in the pipeline or are getting researched out.

# References


- Cyber Security and the Role of Intelligent Systems in Addressing its Challenges, Yaniv Harel, Irad Ben Gal, ACM Transactions on Intelligent Systems and Technology , ACM,Volume 8Issue 4July 2017 .
- Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation Ekta B Jadhav , Mahipal Singh Sankhla , Rajeev Kumar.Journal of Seybold Report,Aug 2020, ISSN NO: 1533-9211.
- Artificial Intelligence and Robotics for Law Enforcement, UNICRI and INTERPOL. (2019). Retrieved from the link http://www.unicri.it/news/files/artificial_intelligence_robotics_law%20 enforcment_web.pdf
- Towards Responsible AI Innovation, Second INTERPOL and UNICRI Report on Artificial Intelligence for Law Enforcement (2020), UNICRI and INTERPOL. (2020). Retrieved from hhttps://www.interpol.int/es/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf
- Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. Dilek, S, et al., 2015. International Journal of Artificial Intelligence & Applications, 6(1), pp. 21-39.
- Discussion Paper - National Strategy for Artificial Intelligence, NITI Aayog.
- Axon (2018). Axon Announces AI in Car Licence Plate Reader. Retrieved from https://www.axon.com/news/ethics/axon-announces-ai-powered-in-car-license-plate reader Axon (2018)
- Using Artificial intelligence to address criminal justice needs by Christopher. (NIJ Journal 280).
- Fake Profile Identification using Machine Learning Samala Durga Prasad Reddy.International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072
- The impacts of artifcial intelligence techniques in augmentation of cybersecurity: a comprehensive review Binny Naik , Ashir Mehta, Hiteshri Yagnik , Manan Shah Aug2021. Springer.
- Artificial Intelligence in the Context of Crime and Criminal Justice Benoît Dupont, Yuan Stevens, Hannes Westermann, Michael Joyce.A Report for the Korean Institute of Criminology December, 2018.
- "Face recognition solution, AI Vision for Delhi police",Case study by INNEFUhttps://www.innefu.com/CaseStudy_DelhiPolice.pdf.
- Crime forecasting: a machine learning and computer vision approach to crime prediction and

prevention Neil Shah1 , Nandish Bhagat1 and Manan Shah2.Shah et al. Visual Computing for Industry, Biomedicine, and Art (2021) 4:9 https://doi.org/10.1186/s42492-021-00075-z.

- Artificial Intelligence: Study Material by IBM-Teacher instruction manual.
- https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime
- Article "Artificial Intelligence in Policing – Use-Cases, Ethical Concerns, and Trends" - https://emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/
- 'Artificial Intelligence in Forensic Science' Siddhant Gupta, Mrs. Vinny Sharma, Dr. Prashant Johri. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072.
- What is Artificial Intelligence? How does AI work, Types and Future of it?https://www.mygreatlearning.com/blog/what-is-artificial-intelligence.
- 'Artificial Intelligence applied to computer forensics', Bruno W.- P. Hoelz, Célia G. Ralha and Rajiv Geeverghese, in Proceedings of the 2009 ACM symposium on Applied Computing, Honolulu, Hawaii, (ACM, 2009), pp 883-888.
- A Review of AI and ML Applications for Computing Systems BY Atul Negi,K Rajesh, Published in: 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19).

# Contact List of BPR&D Officers

| Name of the Officer | Ph. No./E-mail ID |
|---|---|
| Dr. Karuna Sagar<br>IG / Director (Mod) | 011- 26782023 |
| Sh Anuj Kumar Singh<br>DIG/Deputy Director (Mod) | 011-26782184 |
| Sh. Navrattan Joshi<br>PSO (Electronics) | 011-26782185 |
| Lt. Col. Ashwani Kumar<br>AD (Mod) | 011- 26782183 |
| Dr. Raveesh Kumar<br>PSO (W) | 011- 26785451 |
| Sh. Sushil Kumar<br>PSO (B&E) | 011-26734931 |
| Dr. M.M. Gosal<br>SSO (T) | 011- 26734815 |

officialBPRDIndia

BPRDIndia

Bureau of Police Research & Development India

bprdIndia

www.bprd.nic.in

Cyberdost

www.cybercrime.gov.in


**NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)**

**BUREAU OF POLICE RESEARCH AND DEVELOPMENT**

Ministry of Home Affairs, Government of India

NH-8, Mahipalpur, New Delhi-110037