



+ AI |

Copyright © Huawei Technologies Co., Ltd. 2019 . All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademark Notice

 **HUAWEI**, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

NO WARRANTY

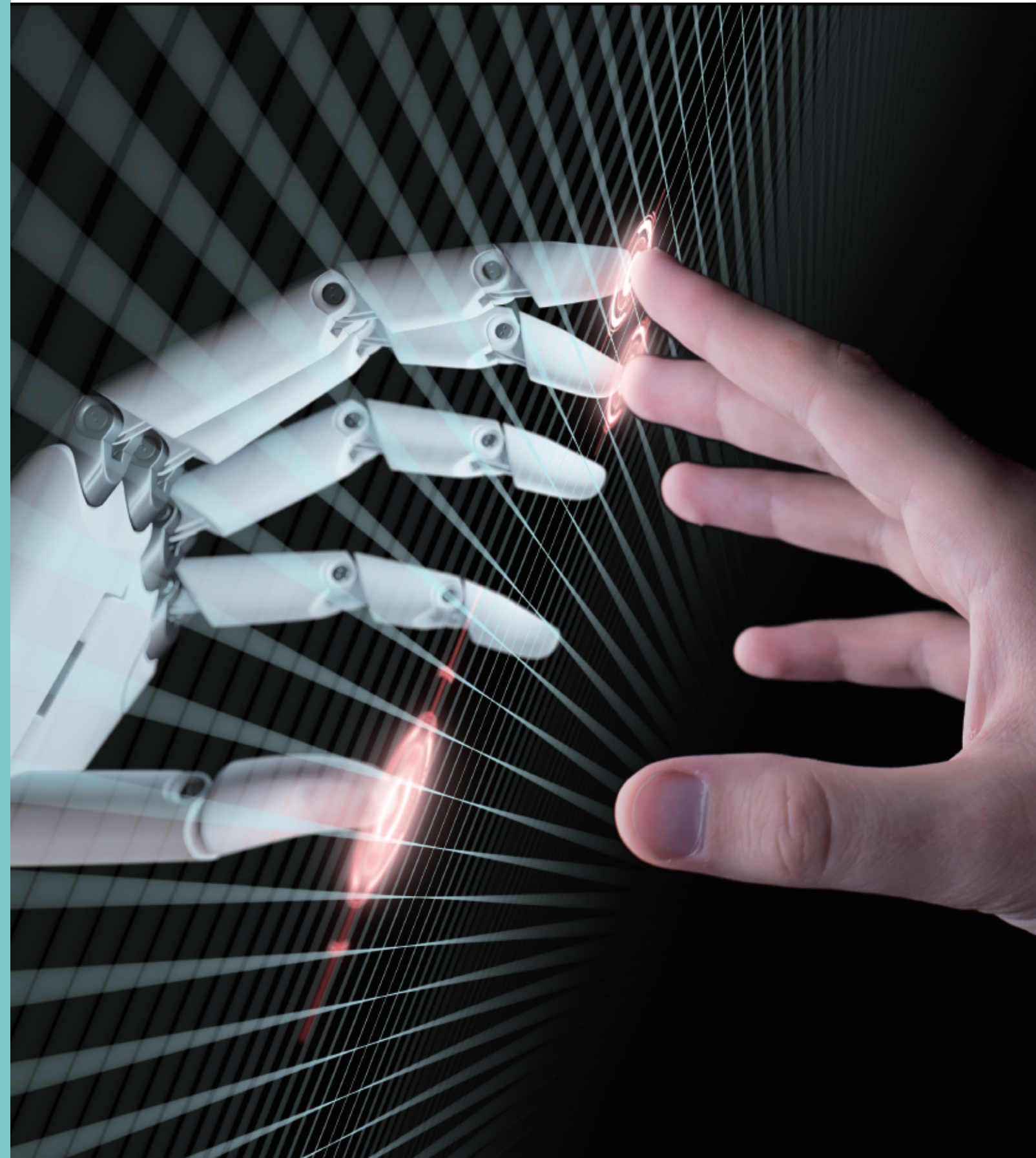
THE CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO CASE SHALL HUAWEI TECHNOLOGIES CO., LTD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS MANUAL.

HUAWEI TECHNOLOGIES CO., LTD.

Bantian, Longgang District
Shenzhen 518129, P. R. China
Tel: +86-755-28780808

www.huawei.com

+AI , Accelerating Collaborative Public Safety





**+AI, Accelerating Collaborative
Public Safety**

TABLE OF
CONTENTS

01	About the Author
03	Collaborative Public Safety
05	Is AI the Answer?
07	Use Cases of AI in Public Safety – The Seven As
13	Seven Concerns regarding AI in Public Safety
14	Seven Implementation Considerations
20	Cases
22	Conclusion

Hong-Eng Koh

Global Chief Public Safety Scientist

Enterprise Business Group

Huawei Technologies Co., Ltd



As a thought leader with decades of global Public Safety & Justice (PSJ) experience, Mr. Koh leads a global team of public safety scientists, experts and business architects to support this major business segment of Huawei. His team engages top public safety agencies globally to help them with high level ICT design to better counter evolving threats. This team, comprising few former public safety officers come from all around world, also advises the product and solution teams to develop state-of-the-art ICT solutions. In addition to offer pre-sales consultancy to customers and support internal solutions development, this team is also helping with partners' development, internal training, and industry marketing.

Mr. Koh is a well sought after speaker internationally and is well regarded in evangelizing the "It takes a Network to Fight a Network" principle in countering crime, terrorism and disaster. In 2014, he created the "Social-Enabled Policing" concept: policing in the age of social networking and crowd-sourcing. In 2016, Mr. Koh authored the paper, "The Road to Collaborative Public Safety"; it's the concept of Public Safety in the age of Digital Transformation. Huawei now has a suite of C-C4ISR™ Collaborative Public Safety solutions to support such transformation.

Prior to joining Huawei for this pioneer global chief scientist position, Mr. Koh spent more than 15 years in Oracle, including Sun Microsystems which was acquired by Oracle. He was the Global Lead in PSJ with similar roles as in Huawei. Mr. Koh and his team contributed to the success of many major PSJ projects globally, such as citizens registry/ID; ePassport; border control system; command, control, and communications (C3) system; traffic incident management system; national disaster warning system; video surveillance system; electronics surveillance system; automated fingerprint identification system; criminal records system; investigation/case management system; court case management system; and prisons management system. Before Sun Microsystems, Mr. Koh was in the systems integration business for a few years and was involved in various mega government infrastructure and application projects, including government-wide networking and messaging projects, and globally acknowledged Singapore's eGovernment projects.

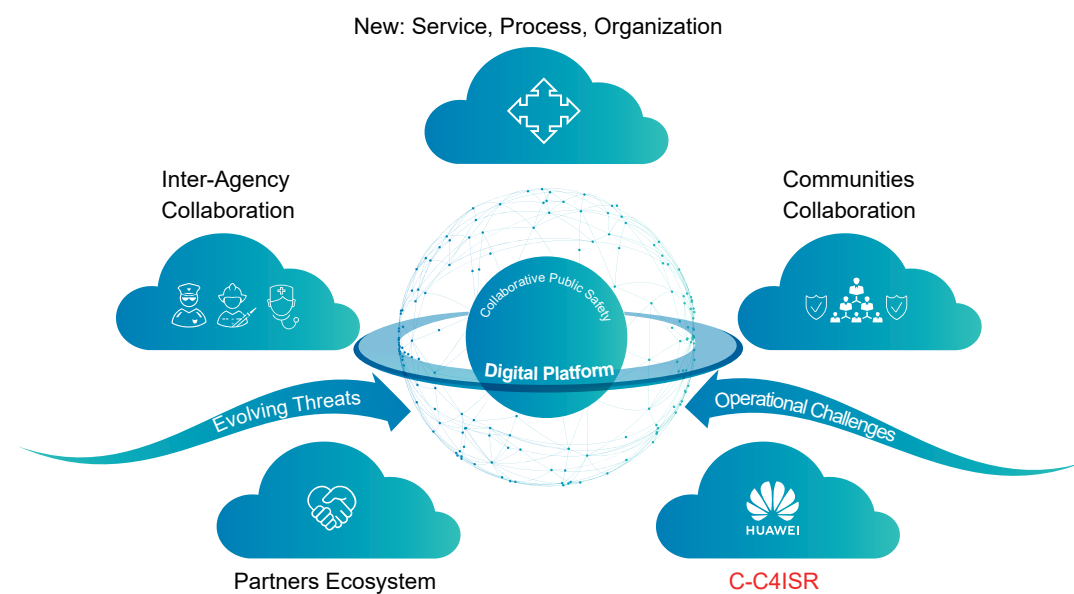
Mr. Koh started his career with the Singapore Police Force (SPF) after graduating under an SPF scholarship. He held various appointments including senior investigation officer, head of crime prevention and community policing, police spokesman, and divisional head of operations and training. His last appointment was as head of the Computer Systems Division, where he led the implementation of various police operational and administrative systems including SPF's first internet project, one-stop change of address system, investigation management system, automated vehicle screening system, resource activation management system, casualty information system, C3 system, and criminal intelligence system. During his years of service in SPF, he received various awards including the Commissioner's Commendation and High Commendation, Good Service Medal, Long Service Medal, and Good Conduct Medal.

Outside his work in Huawei, Mr. Koh is a Vice President of the Society for the Policing of Cyberspace (POLCYB), an international nonprofit society that promotes global partnerships with international criminal justice and corporate agencies to combat and prevent cyberspace crimes. He is also on the expert panel of the Geneva based Global Initiative Against Transnational Organized Crime. In 2014, Mr. Koh was voted by the USA based SecurityWorld as the world's top 12 market influencers in physical security and video surveillance.

Mr. Koh graduated from the National University of Singapore with an Honors Degree in Mathematics. He obtained his MBA with Distinction from the University of Leeds (UK) and a Specialist Diploma in eCommerce from the Nanyang Polytechnic (Singapore). He lives in Singapore with his wife and two children.

Collaborative Public Safety

Since 2016, Huawei has promoted the need for public safety agencies to embrace digital transformation, referring to it as Collaborative Public Safety. Evolving threats against public safety and operational challenges means that agencies are not able to fight these threats and overcome such challenges alone. International and national collaboration is vital. The latest technology provides new methods of organization, processes and services to better achieve public safety. More importantly, as in the digital sharing economy, agencies need to use platforms to reach out to the communities and collaborate with them to prevent, detect, respond and recover from threats. In 2017, Huawei launched a suite of C-C4ISR capabilities and solutions to enable Collaborative Public Safety.



Recently consulting and technology companies, as well as public safety agencies, have begun to promote the need for digital transformation in public safety. However, evolving threats against public safety are increasing and operational challenges are worsening. Examples include:

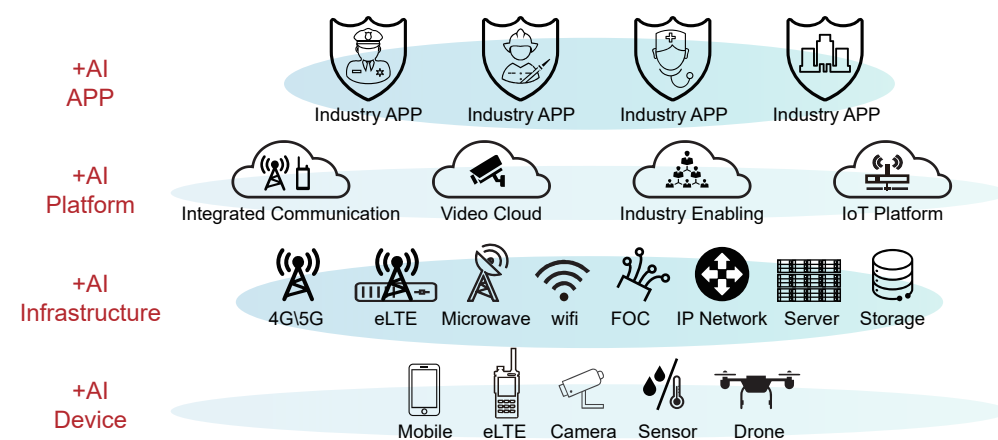
- Well educated people being radicalized online to support terrorism.
- Use of drones to smuggle drugs, and even the attempted use of drone to assassinate the Venezuelan President.
- Predators using popular games/app to groom children, and child abuse imagery has been found within blockchain.
- Critical security flaws in widespread industrial software putting power plants at risk.
- Agencies are still working "in silo" - not sharing critical information.
- Criminals are increasingly countering facial recognition.
- Legacy technologies holding up public safety operations.

Is AI the Answer?

Digital transformation may seem inaccessible, but it is essential to avoid future disruption. Public safety agencies need to accelerate their adoption of Collaborative Public Safety. Even “greenfield” agencies (those with no previous major technological projects) can embrace digital transformation. In fact, these agencies have the advantage of “leap-frogging” legacy technologies, as they start afresh with the latest systems.

Is AI the answer to accelerating the digital transformation of public safety? The short answer is yes. Yet an agency must overcome several obstacles before implementing AI. In my 30 years of public safety experience, firstly as a frontline law enforcement officer, and later designing technologies that enable public safety, I know that agencies and companies often simply follow the latest trends. For example, a software company might be quick to label itself as specializing in business intelligence, then decision-making support, then in providing visual analytics, or big data and now AI! Almost all video analytic companies I have come across recently position themselves as AI companies. This leads to a confusing question; can underlying technologies be rapidly changed?

For AI implementation to be feasible and beneficial, there is a need to look at different perspectives. Importantly, from a technological angle, where there is a need to understand that AI can take place at different technological layers.



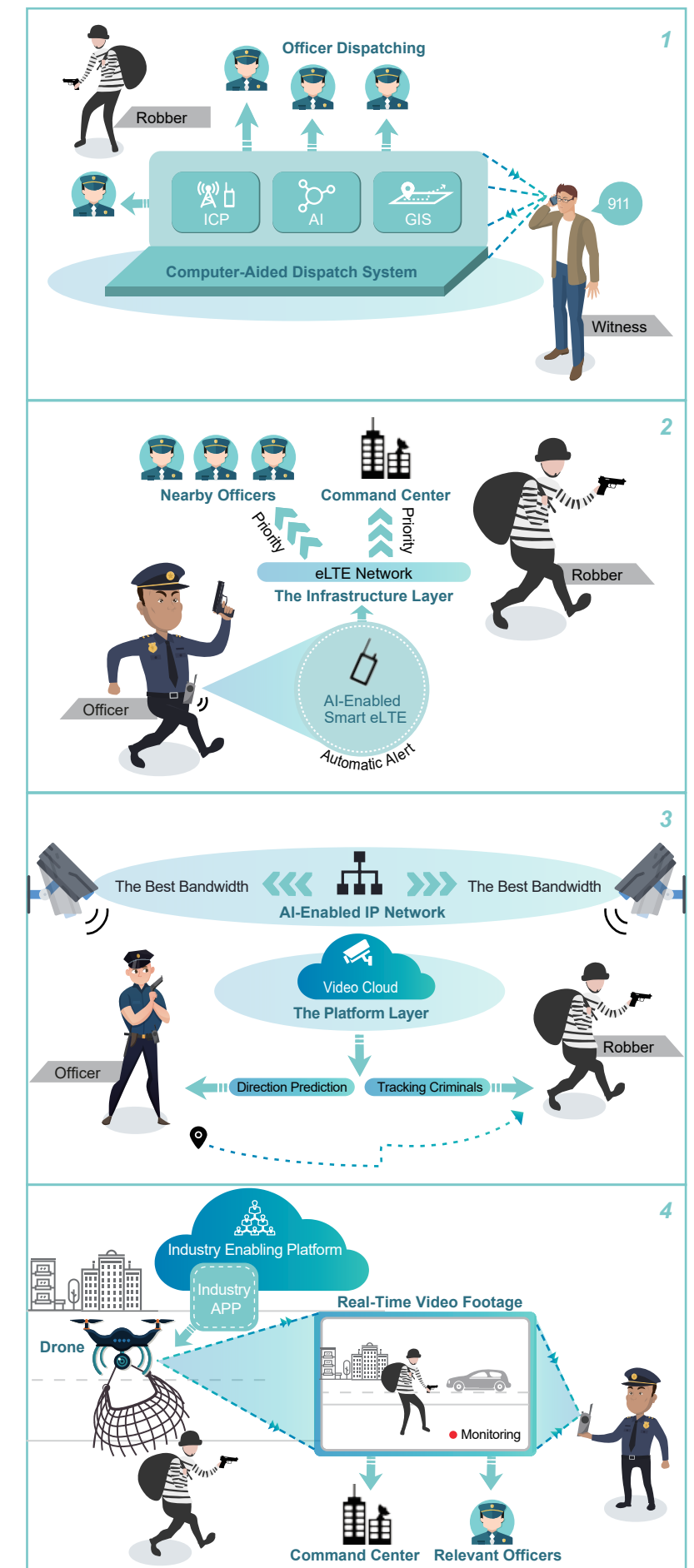
This scenario explains the uses of AI at multiple levels:

1 A man witnessed a bank robbery and the robber, carrying a gun, ran away. He dialed 911 to report the crime. The Computer Aided Dispatch System, an industry app, and the underlying Integrated Communication Platform (both AI-enabled) received the call and autonomously asked for relevant information (without a human operator). The same system and platform were able to automatically dispatch available officers in the vicinity to proceed to the bank and to look for the robber.

2 A nearby officer saw the suspect, who then fired his gun at the officer. The officer, while constantly looking for cover to protect himself, drew out his gun and gave chase. The AI-enabled smart eLTE multimedia critical communication device automatically sent out an alert to the command center and other officers in the vicinity. At the infrastructure layer, the eLTE network was able to grant priority to that eLTE device to make sure it was always online with good bandwidth.

3 With the officer's location known real-time, nearby cameras automatically turned toward the officer and the suspect. An AI-enabled IP network ensured that these cameras had the best bandwidth for high-resolution video streaming. At the platform layer, the Video Cloud was able to track the suspect and even predicted the direction he was heading.

4 Another industry app running on the Industry Enabling Platform automatically launched a drone to intercept the suspect, and sent real-time video footage to command center and relevant officers. The autonomous drone even launched a net automatically to capture the suspect.

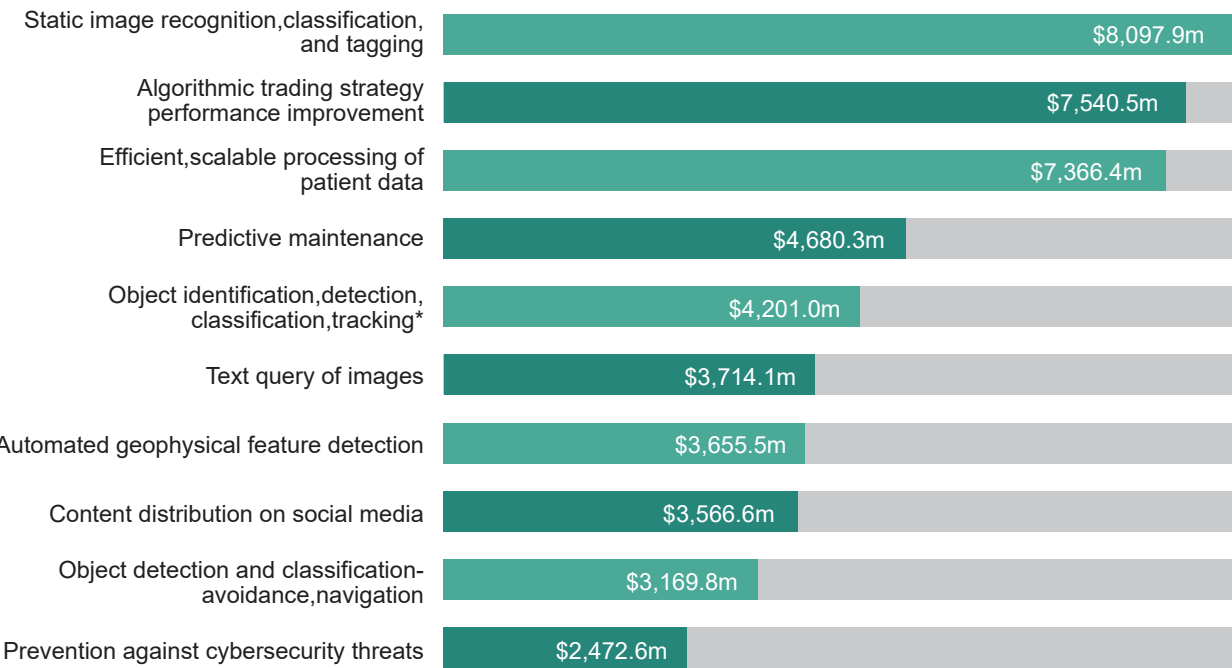




Use Cases of AI in Public Safety – The Seven As

The above scenario is just a single example of the use of AI in public safety. Just like any technological development, it needs to start with a problem we want to solve or an outcome we want to achieve. Many online articles on the use of AI in public safety are too prescriptive. The only shared feature between different public safety agencies, especially internationally, is their mission statement. Their laws, organizations, procedures, people, budget and technological systems are different.

We need a guide for public safety agencies to refer to in order to plan their AI implementations. In terms of online AI case studies, I found that “The Future of AI” by Martin Armstrong is especially useful since it puts a “price tag” on use cases.



<https://www.statista.com/chart/6810/the-future-of-ai/>

The Future Of A.I. Forecasted cumulative global AI revenue 2016-2025, by use case (USD)



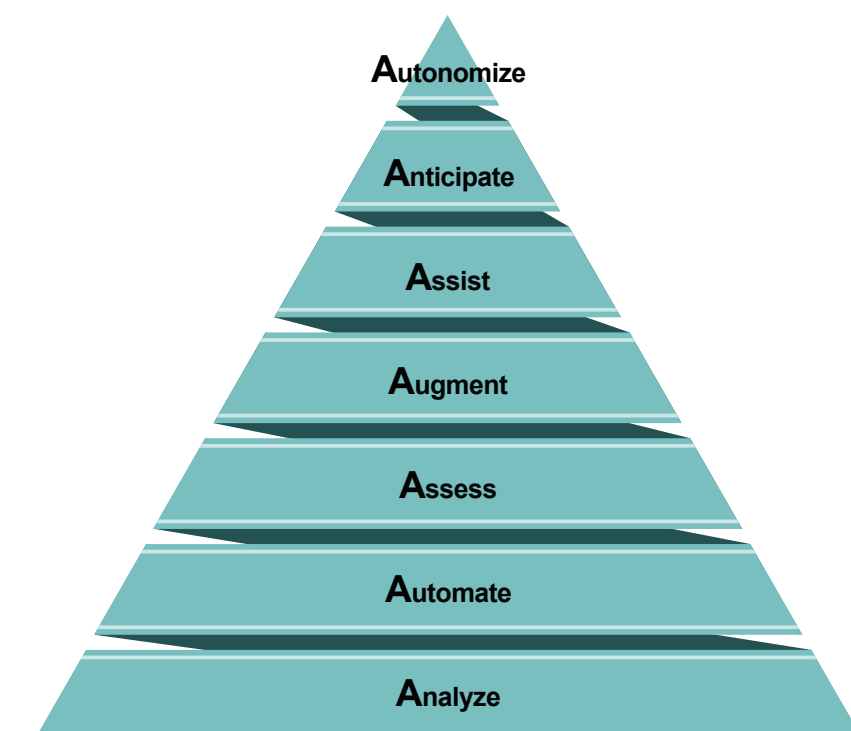
Although the use cases are for all industries, note that eight out of 10 are relevant to public safety:

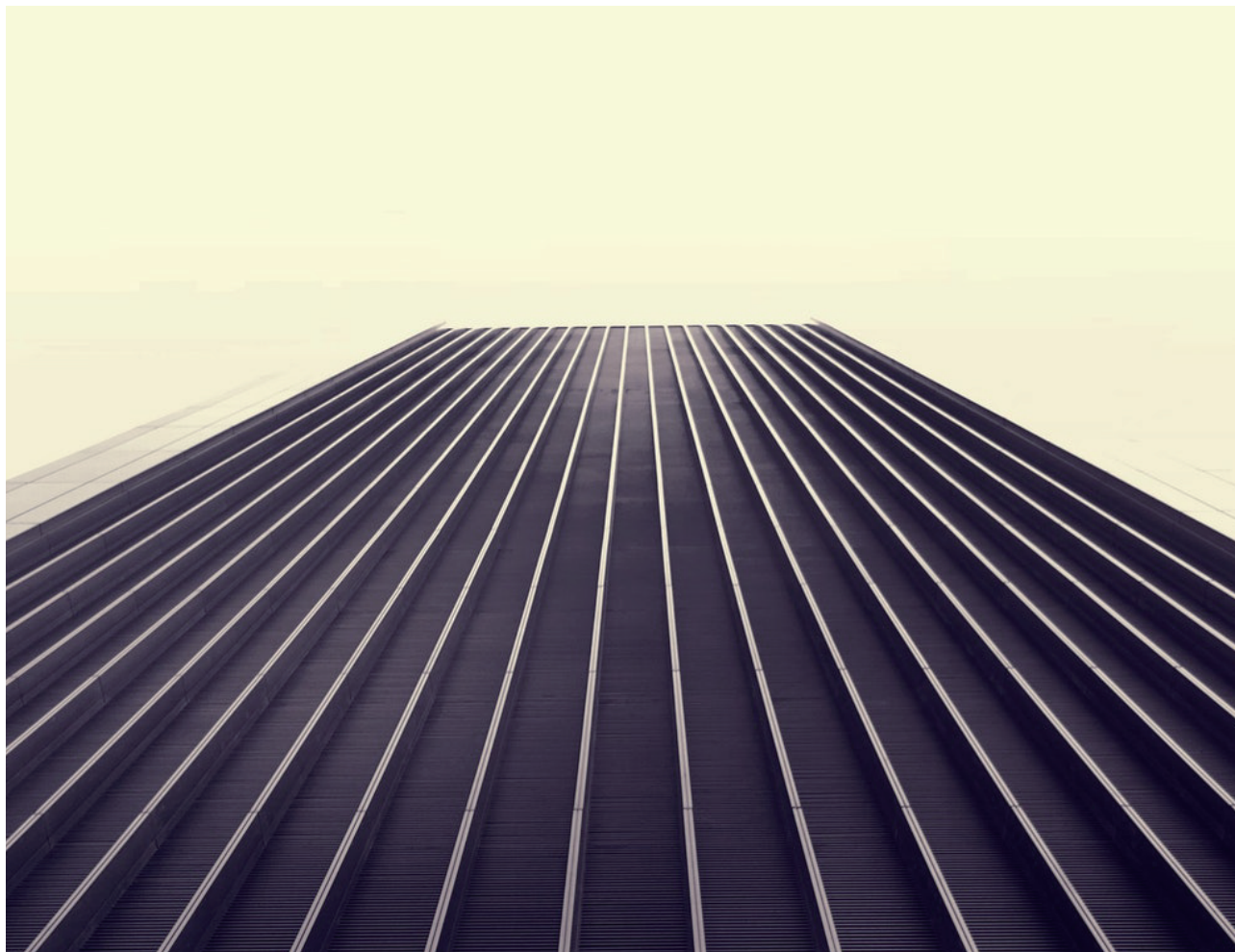
- ① Static image recognition, classification, and tagging: With increasing number of photos/videos from social media and surveillance cameras, such analysis and tagging are crucial in solving and even preventing unlawful acts.
- ② Predictive maintenance: Public safety agencies require much equipment, from guns to vehicles and special rescue equipment. Ordering resources ahead of time increases efficiency.
- ③ Object identification, detection, classification, and tracking: Similar to the static image recognition mentioned above, the analysis and tracking of real-time moving objects is crucial. Object here can refer to a person, mobile phone, stolen property, vehicle, weapon, or even a bomb.
- ④ Text query of images: for both a post-event search or pre-event big data analytics, the need to convert images to textual data is important throughout the lifecycle of public safety (prevention, detection, response, and recovery).
- ⑤ Automated geophysical feature detection: The four important entities in public safety are People, Objects, Locations, and Events. Whether it is a verbal description by the victim about a location, or evidence found in cyberspace, geophysical identification will be a great bonus.
- ⑥ Content distribution on social media: In line with Collaborative Public Safety, collaboration with the communities applies to social media too. Agencies need to win the trust of communities before leveraging them to help jointly uphold public safety.
- ⑦ Object detection and classification - avoidance, navigation: This is relevant when public safety agencies start to use drones and even robots.
- ⑧ Prevention against cybersecurity threats: This is particularly relevant for the public safety industry so that public safety agencies can protect their very sensitive data, but also, in general to reduce cybercrimes.

In addition to the above list, I feel that we should discuss three other uses of AI in public safety:

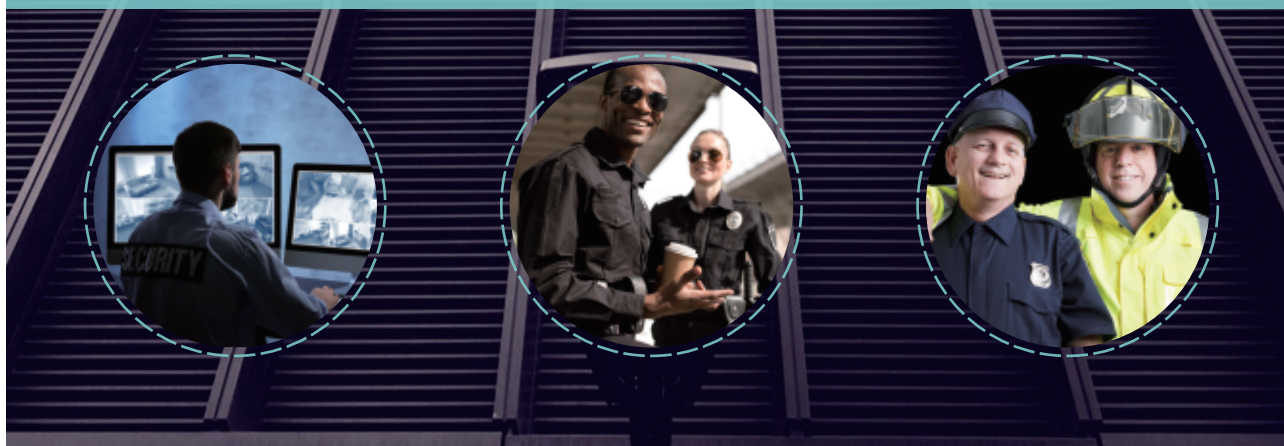
1. Language & sound processing: Ranging from automatic call taking to lawful communication interception, such capability is crucial to public safety.
2. Planning: From crime prevention policing to major event security assurance, and from emergency management to post-event investigation, public safety agencies require a lot of planning regarding resource mobilization and deployment.
3. Reasoning: The best way to prevent crime is to understand when, where and why past crimes occurred. Reasoning capability will prove an incredibly useful tool in crime prevention.

Although comprehensive, the above AI use cases are driven by technological capabilities. We need a generic framework of actionable use cases for different public safety agencies to write their own AI roadmaps. This planning will be based on the laws empowering them, their organizations, procedures, people, technological systems, budget, and more importantly, their own requirements and desired outcomes. I propose the use of this seven As framework to help public safety agencies identify and prioritize their AI use cases:





The seven As model serves as a generic framework of actionable use cases for public safety agencies to consider when planning their future AI usage. Here are more public safety scenarios, which illustrate the possibilities for AI using the seven As: ►►



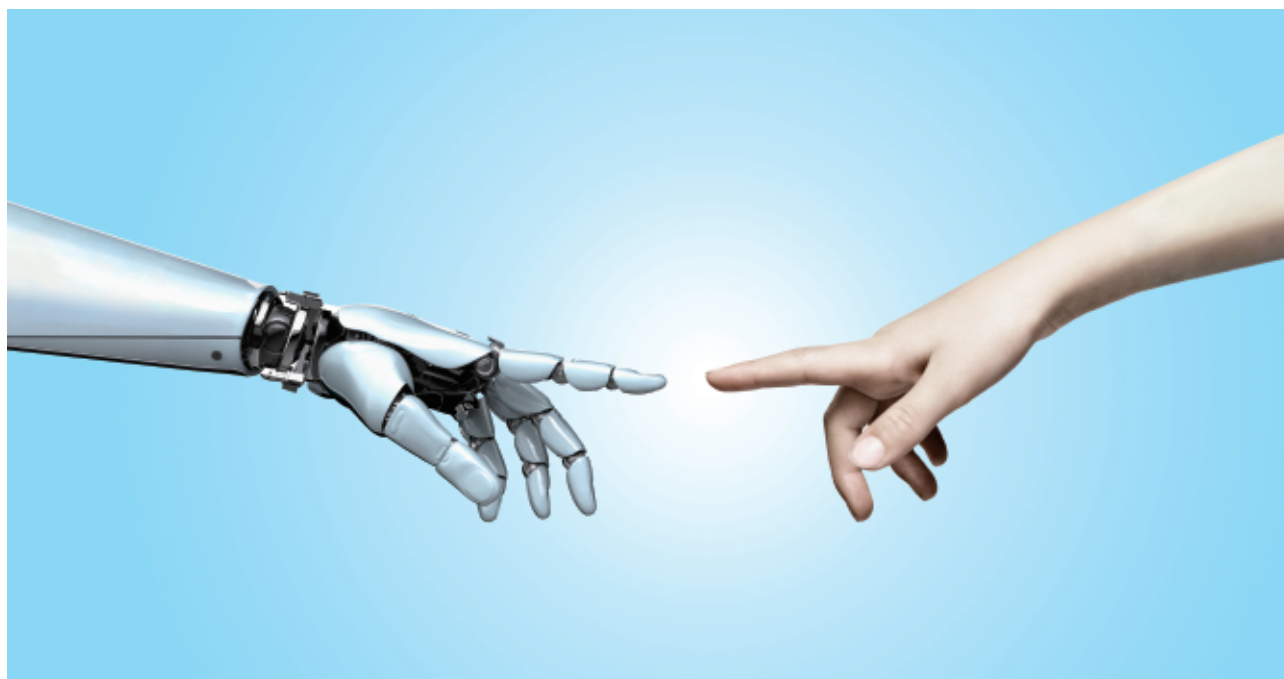
This framework does not represent a mandatory seven-step process for public safety agencies to implement AI applications, and these capabilities do not have to be put into place sequentially. This framework does rank the difficulty in implementing AI applications from “Analyze” to “Autonomize”:

1. **Analyze:** The most basic and easily achieved capability, from analyzing textual data, photos, video, audio, and even sensory data. Such analysis should create textual conversion, description and tagging on the data item being analyzed. This capability addresses Who, What, When and Where.
2. **Automate:** Public safety involves a lot of routine procedures which can be automated through AI applications. Examples include daily crime report generation, the skills-based deployment of officers, crime scene photos classification, investigation summaries, and vehicle rostering.
3. **Assess:** This is where AI implementations start to get interesting. This capability is beyond the analysis of data items, and involves an assessment of the bigger picture. It is beyond knowing who, what, when and where, assessment needs to address the why and how, such as why a series of similar crimes was committed in a neighborhood, or how a person is radicalized to support terrorism.
4. **Augment:** Laws govern the vast majority of all public safety operations; but many decisions have to be made by frontline officers using their situational assessment, knowledge and experience. This is why in a few industries, AI is more commonly known as Augmented Intelligence. It is a complement to – not a replacement of – human intelligence. It is about helping humans become faster and smarter at the tasks they are performing. For example, providing knowledge of crime prone areas AND the location of past criminals in those areas, so that the officers concerned can make a better informed decision. Such augmented knowledge must be provided to the right officer at the right time and at the right place.
5. **Assist:** This is where the human has an AI assistant, likely to communicate in natural language (as opposed to data and visualization). Using the same example used to demonstrate the “Augment” principle, here the assistant can suggest a route for the officer to patrol, including the places to visit, and the people to check on, based on priorities, urgent dispatches, and cost-benefit analysis.
6. **Anticipate:** Using AI applications to anticipate, meaning to predict crimes, riots, traffic accidents, and even whereabouts of suspects.
7. **Autonomize:** Not exactly Robocop, but a system including software applications, drone and vehicle capabilities. Basically, a robot that operates autonomously with no or little human intervention. We can consider whether it should be armed, too, but this involves legal and ethical discussion.

- **Border Surveillance & Protection:** Analyze intrusion by humans or vehicles; Assess whether it is a wild animal; Anticipate hot spots for smuggling; and Autonomize the launch of drones.
- **Hazardous Materials (HAZMAT):** Automate the tracking of vehicles carrying HAZMAT; and Augment human with real-time information on HAZMAT vehicle going near VIP vehicles or critical infrastructure.
- **Child Exploitation:** Analyze social media content and Assess whether it is an attempt to groom children for sexual exploitation; Assist humans with alerts on such predators; and Anticipate predators’ next move.
- **Dangerous Incident:** Analyze social media content and Assess the situation together with video data for potentially violent incidents; and Anticipate where such incidents are likely to take place.
- **Online Radicalization:** Automate acting as targets for such radicalization to track down the perpetrators; and Assist humans by chatting with such perpetrators.
- **Disaster:** Assess the destroyed areas with the most survivors; Augment humans on routes and the availability of transportation for search and rescue; and Anticipate future disasters.
- **Command, Control & Communication:** Automate the preventative crime patrol planning; Assist humans with call taking; and Autonomize the dispatch of first responders.
- **Counter Drone:** Analyze for hostile drones; Anticipate the location of the pilot; and Autonomize the counter strike of the hostile drone.
- **Public Warning:** Automate the testing of the system; and Assess the risks and Autonomize the warning broadcast.
- **Displaced Survivors:** Assist humans in the triage area to determine the level of treatment/assistance for survivors; and Anticipate the need for essentials such as water, food, and shelters.
- **Physical & Digital Crime Scene:** Automate the archiving of evidence; and Assist humans with unusual entities at the crime scene.
- **Prisons & Corrections:** Assess the suitability of early parole of prisoners; and Anticipate fights in prisons.

Seven Concerns regarding AI in Public Safety

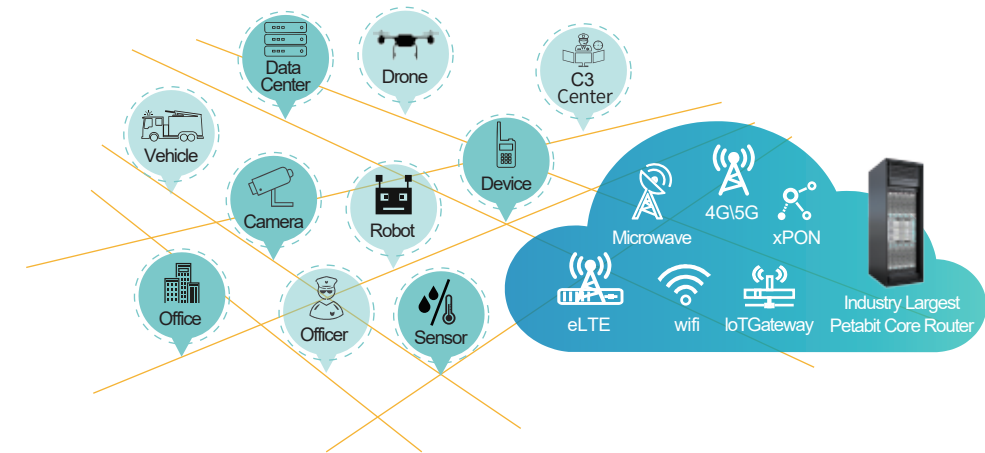
1. Over-Expectation: While not “Robocop”, some of my above examples may still prove optimistic, especially for “greenfield” agencies. An agency needs to start with a vision and an implementation roadmap – to literally think big start small - using the seven As framework to prioritize their requirements and desired outcomes.
2. Internal Resistance: A big consideration is the fear of losing one’s job, so the agency needs to assure its staff that they will be upgraded to do more skilled work. It is also important to involve staff in AI implementation, as their knowledge and experience are crucial in formulating algorithms.
3. Public Confidence: Fear of the unknown may lead to the loss of public confidence. Open and timely communication with the public is crucial, especially in gaining their trust and involvement with Collaborative Public Safety.
4. Privacy: AI applications not only analyze a lot of data, but develop profiles and opinions on individuals too. Protecting privacy is a necessity to uphold public confidence and avoid discrimination.
5. Algorithmic Biases: There are already cases of AI systems learning from humans and becoming racist, sexist, and prejudiced. Transparency in algorithms and a regular review of algorithms may be required.
6. Laws & Ethics: Use of AI systems must adhere to laws. The more difficult consideration is whether the use of AI is ethical, such as the autonomous killing of an armed criminal who is a danger to others, for example. An agency may need to prepare a set of ethical guidelines on the use of AI.
7. Implementation: While AI is more than just an ICT project, we still need to look at the technological implementation issues, addressed in the next section.



Seven Implementation Considerations

1.Connectivity

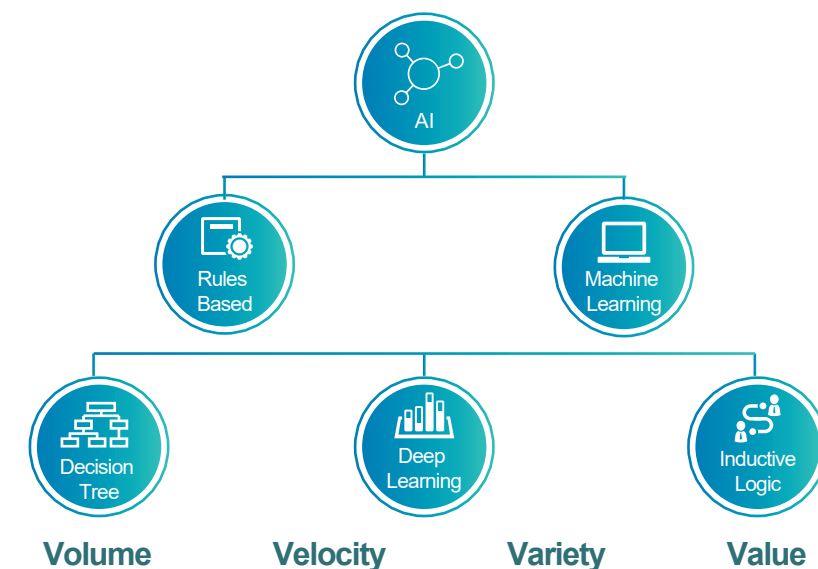
While overlooked, connectivity is crucial. Just like human’s five senses to collect “data” before the brain makes a decision, AI systems need many different data sources for optimal processing. Wireless connectivity is especially important for mobility, so that AI systems can receive data from and transmit instructions to the thousands of devices and sensors.



Huawei has the most comprehensive selection of connectivity technologies, wired and wireless, to connect to a wide variety of data sources, and the industry’s largest Petabit core router to manage this huge volume of data.

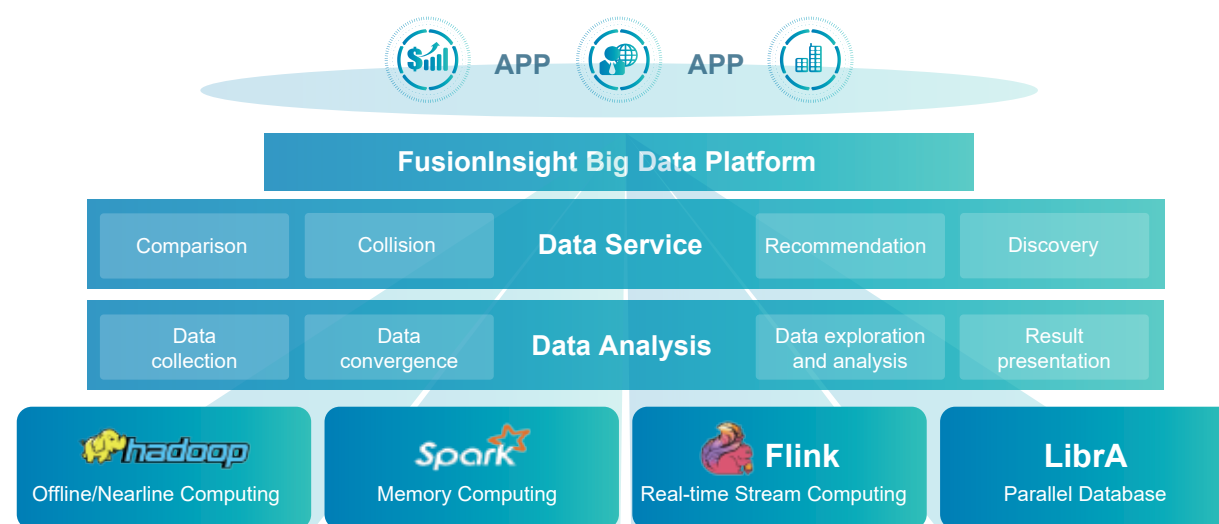
2. Big Data

AI can be achieved through rule-based hardcoding or machine learning, in which a machine can learn through many ways including decision tree, inductive logic, and deep learning. The shared feature of all these techniques is the requirement for high volume, high velocity, high variety, and high value data – Big Data:



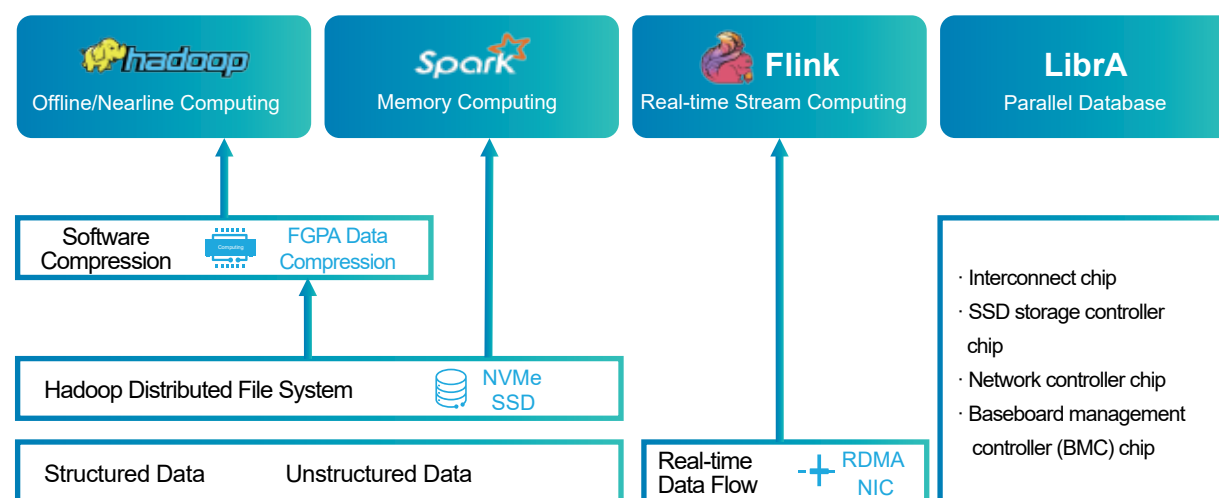
Huawei's FusionInsight big data platform offers an extensive suite of services, including Hadoop, Spark, Flink and LibrA. The platform even has its over 200 data models/algorithms specifically designed for public safety, allowing partners and customers to rapidly develop their own applications. This platform is good for the four typical Big Data scenarios: ▶▶

- Offline/near-line computing with a large data volume with few low latency requirements;
- In-memory computing with moderate low latency requirements;
- Real-time stream computing with strict low latency requirements;
- Massive structured data analysis.

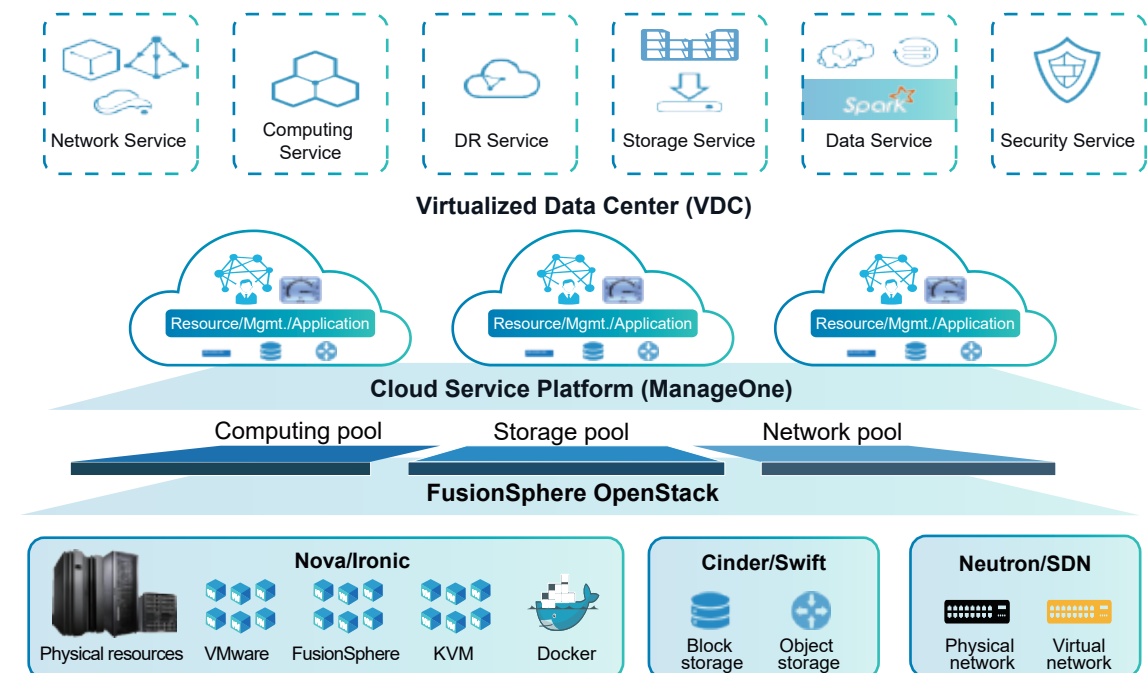


3.Computing Power

Big data requires big computing power. AI is essentially data-driven, so output needs to be calculated quickly and accurately. Huawei uses specialized hardware to better support the four scenarios mentioned earlier:



In addition to Huawei's hardware innovation, the FusionInsight big data platform can run on Huawei's cloud technologies for better resource pooling (computing, storage, and network), and on-demand flexible self-services with ease.



4.Enabling Platforms

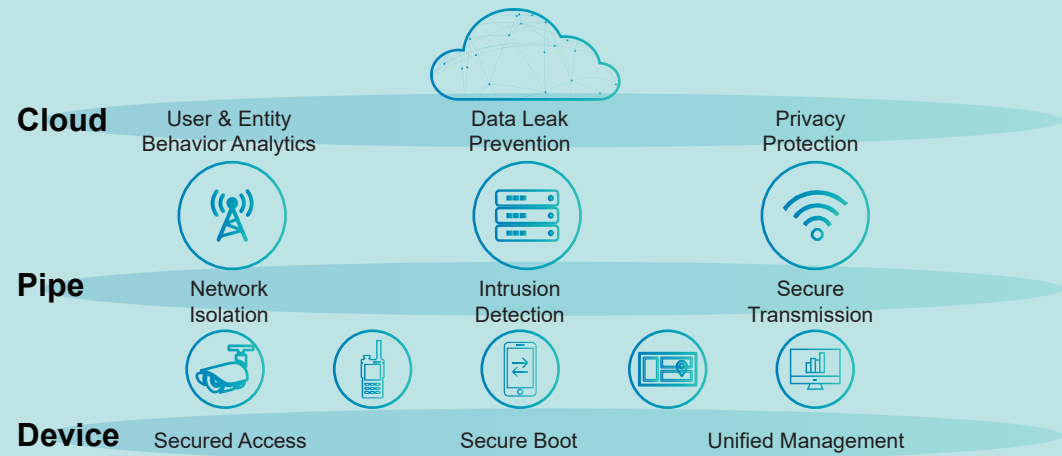
With AI applications, the possibilities are almost endless, and public safety agencies can therefore use the 7 As framework to conceptualize and prioritize their application of AI. We need enabling platforms to make it easier for AI applications to be rapidly developed, without worrying about hardware integration and performance. In addition, we need platforms which don't require connections to other data sources, and which have common components ready to use outside of applications. Huawei's suite of C-C4ISR platforms meet these needs and enable Collaborative Public Safety:



These platforms, together with partners' applications are for all kinds of cities. There are tens of thousands of cities with a population of less than one million. The safety of medium-sized cities is also important, and we need access to a variety of data to provide more accurate insights for an effective AI program. This is why Huawei offers Safe City Compact solutions, which can also be used by medium-sized cities.

5.Cyber Security

With the massive volume of data, and mostly sensitive data, public safety agencies have to take extra precautions to safeguard their cyber security. Any data leaks are sure to breach privacy protection and lower public confidence. Worse still, data manipulation can lead to undesirable and even incorrect AI outcomes. Huawei takes security very seriously through our cyber security strategy and approach, especially the Integrated Product Development processes designed by IBM to assure the cyber security of Huawei's products, where independent security verification are carried out from product conceptualization to development to lifecycle maintenance. Separately, Huawei offers an AI-based Unified Security solution to detect, predict and mitigate cyber threats.



6.Continuous Innovation

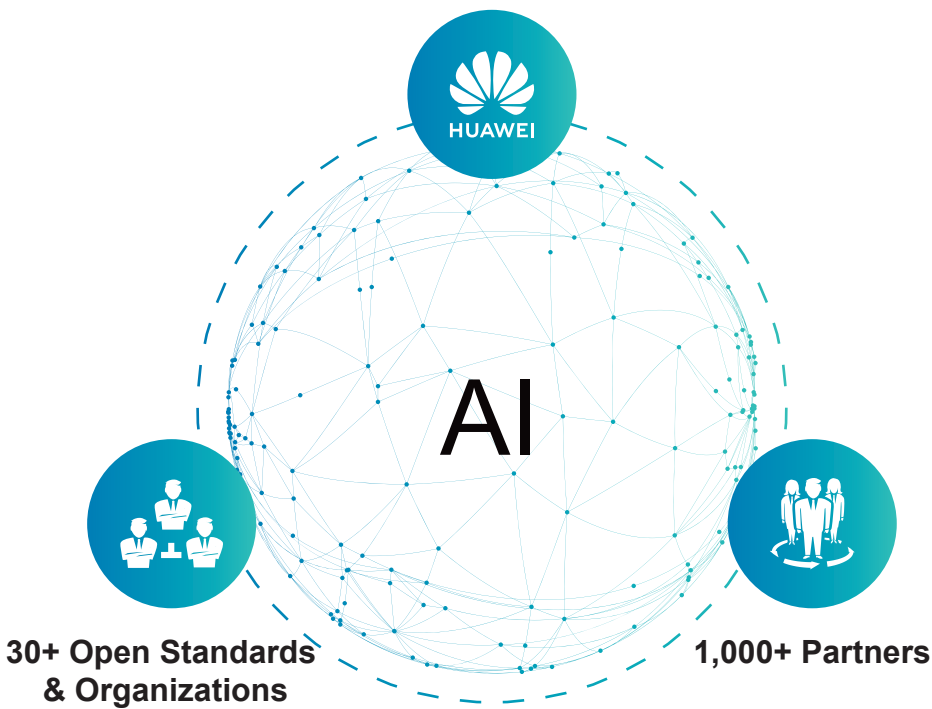
AI Implementation is a journey; it relies on continuous innovation to achieve the best outcomes. According to the World Intellectual Property Organization, in 2017 Huawei was the top company (across all industries) in terms of the number of patents applied for at 4,024, applying for over a thousand more patents than their nearest rival. Examples of Huawei's ongoing innovation includes the two recently launched AI-related products: a Software Defined Camera and Intent-Driven Network, which are part of the AI+ Device and AI+ Infrastructure respectively mentioned earlier.

7. Industry Ecosystem

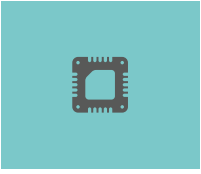
AI implementation requires an entire ecosystem. Implementation needs to be undertaken openly to avoid vendor lock-in. Huawei supports and has adopted more than 30 open standards, and has over 1,000 partners providing applications on our platforms. These partners are supported by our international OpenLab facilities.




Huawei's Capabilities




Huawei's capabilities as a leading ICT company include a complete, full-stack AI portfolio, which covers all scenarios from devices to connectivity to cloud platforms. The range of technologies includes:




The Ascend series of specialized chips based on unified scalable architecture;



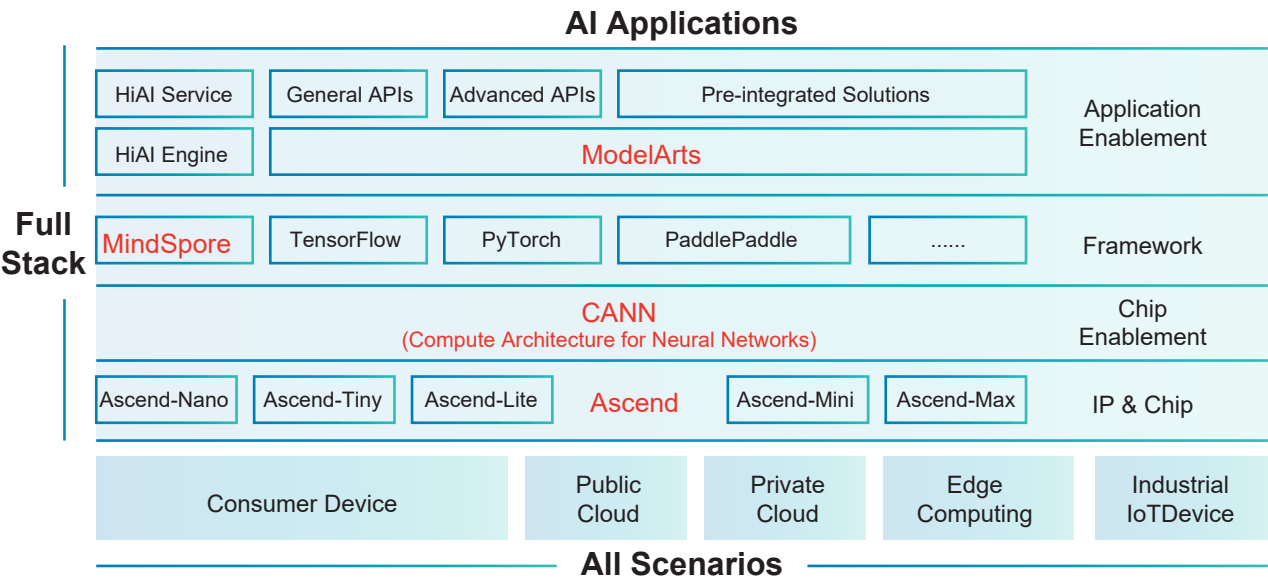
The CANN chip operations library and highly automated operational development toolkit;



The MindSpore unified training and inductive framework (for device, edge, and cloud computing);



Application enablement for end-to-end services (ModelArts), multiple-level APIs, and pre-integrated solutions such as the public safety solutions behind our C-C4ISR capabilities.



With over 6,000 Huawei professionals dedicated to public safety (including many with frontline public safety operational experience) we are in a good position to help design the architecture needed for AI implementation. Beyond technology architecture, we can also assist in business architecture, data architecture and application architecture.

Cases

AI is disrupting existing business models to create new opportunities for global public safety. To date, more than 230 cities in over 90 countries have deployed our public safety solutions. What's more, an increasing number of cities have introduced AI technology into their solutions. A few examples of cities that are embracing the future of AI are included below.



In Kenya

Safe City solutions based on visualized critical communications and AI technologies helped the police shorten their response time by 60%, reduce the annual crime rate by 46%, and improve overall security. As a result, local tourism developed rapidly, growing 14% in 2016.

In Mauritius

An AI-enabled intelligent video cloud solution will greatly improve the efficiency of video analysis for public safety incidents. The solution also helped to optimize traffic management and reduce traffic accidents.

In Pakistan

A Safe City solution based on the intelligent image recognition technology was used to construct license plate recognition system for cars, with a recognition rate of 90% in daytime. Since the system was deployed, the handling time of explosive cases has been reduced from 45 days to 2 days, and the incident response time has been shortened from 30 minutes to 10 minutes.

Conclusion

The digital transformation of public safety (Collaborative Public Safety) must be implemented, or the sector risks facing disruption due to evolving threats and operational challenges. It is time to activate intelligence to AI-enable and accelerate Collaborative Public Safety.

Requirements and desired outcomes dictate the application of AI. The 7 As framework can help an agency to identify and prioritize what they need AI to do: Analyze, Automate, Assess, Augment, Assist, Anticipate, Autonomize.

When an agency is ready to begin its AI journey, it should bear in mind the seven concerns outlined above: Over-Expectation, Internal Resistance, Public Confidence, Privacy, Algorithmic Biases, Laws & Ethics, and Implementation.

In addition, we need to consider the following seven areas when it comes to the implementation of AI projects: Connectivity, Big Data, Computing Power, Enabling Platforms, Cyber Security, Continuous Innovation, and Industry Ecosystem.

