Artificial Intelligence and its Applications in Security

David Quinn and Janice Goldstraw-White
July 2022

G4S Academy

CONTENTS

I INTRODUCTION

The artificial intelligence (AI) sector (that is intelligence demonstrated by machines, as opposed to the natural intelligence exhibited by humans or animals) is estimated as having a net worth of £15.6 billion to the UK economy[I] and spend on AI technologies is predicted to rise to £35.6 billion by 2025[II]. These figures give a clear indication that the advancement of AI applications is more than a passing phase albeit that adoption rates in the UK vary greatly between industries and appear highest in the finance, IT and legal services areas; compared to the security sector which lags behind.[III]

The Covid-19 pandemic was a game changer for the security sector. For example, security personnel were not only required to carry out their normal duties, but as frontline workers, they were also charged with ensuring compliance with Covid restrictions (such as mask wearing, marshalling queues and taking temperatures), as well as being required to monitor access to buildings more closely and particularly occupancy rates[IV]. The use of technology, including AI, sometimes played a significant part in carrying out these additional tasks.

Contained in this article is a discussion about what exactly AI is, some key benefits, and where it fits into a security solution, giving real-life working examples and case studies. There is also consideration about some of the constraints of AI which impede its development, and finally, there is a look to the future as to what AI could attain, if some of these barriers are overcome and technical progress continues.

2 WHAT EXACTLY IS ARTIFICIAL INTELLIGENCE?

AI was founded on the assumption that human intelligence could be simulated by machines[V,] however, to date, AI does not 'think' or 'create', instead it computes, processes, and applies (or on some instances, makes) rules. It is therefore relatively inflexible, and because it does not have the capacity for human understanding, it cannot adapt like a person to changes in dynamic circumstances[VI]. It is sometimes confused with the term 'automation', which aims to simplify and speed up common repetitive tasks to increase productivity and efficiency, with little or no human involvement. AI aims to use machine learning to solve problems and accomplish some tasks that would too great, too complicated, or take too long for the human brain to process[VII].

There is no one agreed definition of AI and this has been the case since its inception. As to why this is, suggestions include that AI is still evolving, that there is a lack of agreement on what exactly 'intelligence' is, that it rarely operates alone, and that sometimes it is difficult to see boundaries with other systems, and finally that sub-fields of AI are not clear cut. However, in broad terms, most definitions see AI as *'the simulation of human intelligence processes by machines, which can learn from experience'*[VIII] and can include human tasks such as visual perception, speech recognition, language translation, and some limited decision-making[IX]. In the security world, ASIS have defined AI as: *'a subsection of computer science that investigates and develops computational approaches and techniques that enable machines to perform tasks that would normally require some level of human intelligence'*. Others clarify that machines could also mean computers and robots, 'which have a humanlike ability to reason and solve problems.'[X]

Perhaps an easier way to look at AI is to see what technologies and processes it includes, most of which have their own branches in mathematical and engineering disciplines. The five most commonly used technologies are: (i) machine learning, (ii) natural language processing and generation, (iii) computer vision and image processing/generation, (iv) data management and analysis, and (v) hardware.[XI] Definitions of these are included in Table A.

Table A – Common AI technologies[XII] [XIII]

Technology	Explanation	Examples
Machine learning	Focuses on getting a system to learn and relate information the way a human would, by using algorithms to detect patterns in previous data and make future predictions and responses. Deep learning is a subset of this and refers to the ability of machines to learn and improve from their experience automatically, without further programming.	• anomaly detection; • deep learning/neural
Natural Language Processing (NLP); Natural Language Understanding (NLU); and Natural Language Generation (NLG)	NLP enables machines to understand the human language (written or vocal) so it can automatically perform different tasks. NLU as a subset of NLP, helps machines understand the intended meanings and context of the text. NLG, another subset, is the process of turning structured data into text or speech.	• chatbots • virtual assistants • machine translation • voice recognition • image captioning

2 WHAT EXACTLY IS ARTIFICIAL INTELLIGENCE?

Technology	Explanation	Examples
Computer vision and image processing /generation	Focuses on getting a system to learn and relate information the way a human would, by using algorithms to detect patterns in previous data and make future predictions and responses. Deep learning is a subset of this and refers to the ability of machines to learn and improve from their experience automatically, without further programming.	• anomaly detection; • deep learning/neural
Data management and analysis	AI processes that are embedded in data management systems, that include database query optimisation to reduce system overload and improve outputs.	• data formatting and processing • forecasting • database query
Hardware	These machines or robots orchestrate and coordinate computations for the AI process using accelerators for fast and high performance.	• autonomous machines • drones • robots • self-driving cars

In order to understand AI it is useful to distinguish between the different types, and there are a number of ways AI can be classified, but two of the most popular are by capabilities and by functions. AI that is considered by its capability is usually referred to by technical specifications and consists of three main categories - Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI), and Artificial Superintelligence (ASI).

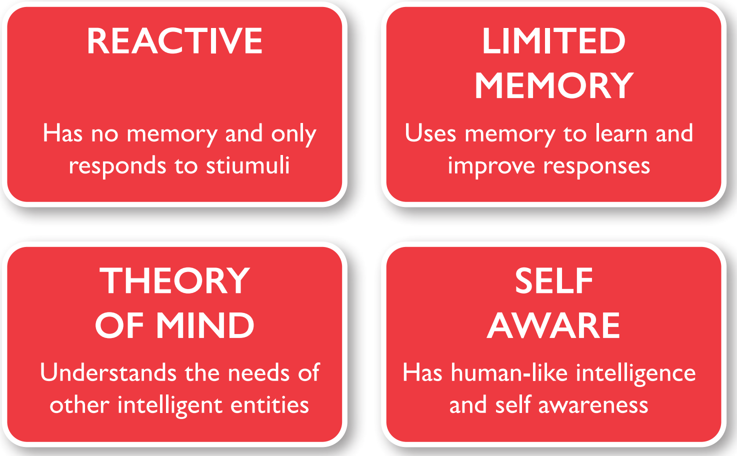
ANI is the only form of AI currently on the market and is very good as performing better than humans for completing repetitive tasks within the arena for which it has been designed. For example, Siri and Google Translate both employ ANI, and it can also be used for face, image and voice recognition tasks, evidenced in recommender systems where it profiles behaviours and matches products or services, such as those used by Amazon, Spotify and Netflix[XIV]. Where two or more systems or techniques of ANI are integrated, this is referred to as Broad AI and scientists are currently exploring this next level. It would be more efficient than ANI and more adaptable, demonstrating advance reasoning, allowing it to performance more sophisticated and cognitive tasks.[XV]

AGI, or ‘strong’ / ‘deep’ AI, as it is also known, is a type of AI which mimics the reasoning skills of a human, but to date, however, is still generally at a theoretical concept. Machines would be able to understand, learn and carry out any intellectual task that a human being could, and apply that knowledge and skill in different contexts[XVI]. This type of AI is expected to be self-aware, and to be able to understand beliefs, thoughts, emotions, expectations of humans, as well as to interact socially, but lacking its own emotion. Such advances are still in the very early stages of development[XVII].

Finally, ASI is more of a futuristic notion of AI where machines equipped with this level of ability would be more than capable of outperforming the most gifted and brightest of humans[XVIII]. It would mean developing systems which had the ability of reasoning beyond human capabilities, as well as building emotional relationships. To do this they would need to not only understand them, but to also summon up on their own, emotions, needs, beliefs and desires.[XIX]

2 WHAT EXACTLY IS ARTIFICIAL INTELLIGENCE?

Moving onto the second main way of classifying AI – by functionalities – this where AI is characterised by its ability to recreate human-like functions and there are four types of AI identified in this way – Reactive, Limited Memory, Theory of Mind and Self-Aware (see Figure 1).



REACTIVE
Has no memory and only responds to stiumuli

LIMITED MEMORY
Uses memory to learn and improve responses

THEORY OF MIND
Understands the needs of other intelligent entities

SELF AWARE
Has human-like intelligence and self awareness

Figure 1: AI types by functionality[XX]

Reactive AI is the most basic form of AI, where machines focus on the current environment and react to it. They do not store past data, nor interact with the world, they just react to specific tasks in an identical way. Examples include spam filters, and chess playing programs.

The next level of AI is Limited Memory and this type can store and use previous data to improve performance and make better predictions to events, in a similar way to which human brain's neurons connect[XXI]. It achieves this by using more complex machine learning models including reinforcement learning – learning through trial and error[XXII]; long short-term memory – predicting the elements in a sequence[XXIII]; and evolutionary generative adversarial networks – algorithm architecture that evolves with modifications[XXIV.] This type of AI is the most widely used and being perfected today and has contributed immensely to the advances in autonomous drive cars.

The remaining two types of AI, when classified by functionality, are still very much in the conceptual stages. Theory of the Mind AI means that AI needs to thoroughly understand people and things within an environment, and to alter its feelings and behaviours accordingly. It means that machines will be conscious, able to think and experience emotions. Developing this advanced technology is challenging, not least that we do not fully understand how the human brain thinks[XXV].

Self-aware AI exists only hypothetically and is an extension of Theory of the Mind. As the name suggests it would not only have human-like intelligence but also display self-awareness. This means it could take cues from humans (and other robots/machines) and react accordingly, but also be self-driven. Machines driven by this type of AI would be far smarter than the human brain and possess their own needs, emotions and beliefs. Researchers are not total in agreement at what point a robot would become self-aware[XVI].

3 ADVANTAGES AND DISADVANTAGES OF USING AI

Adopting AI technology can have a number of positive benefits for organisations, not least that it can increase their overall efficiency. By working 24/7 without interruption, breaks or downtime, compared to a human workforce, it can enhance productivity through making processes faster and smarter. It can perform repetitive tasks accurately, whereas humans might get bored, tired and lose concentration, leading to errors[XXVII]. Furthermore, AI technology can be deployed across a number of industry sectors and used at different levels of capabilities[XXVIII].

Besides assisting in routine and mundane jobs, it can also enable performance of more complex tasks, which is useful in decision-making, where not only does AI technology make decisions faster, filtering out some of the issues that might delay humans, such as emotional and practical factors, but it can use deep learning to handle vast amounts of data. This enables it to train itself and use this learning to categorise the data and build models to make more accurate future predictions[XXIX]. A further advantage of employing AI technology to undertake tasks is it can take risks rather than exposing humans to these. This could include using robots for defusing bombs and also in assisting governments and relief agencies by using data to predict natural and manmade disasters[XXX].

As noted, there are some disadvantages of using AI, not least that the start-up costs can be huge, depending on the level of intelligence and complexity an organisation is trying to achieve, the type of devices and software being used, and the amount and quality of data intending to feed the system[XXXI]. In addition, machines and technology will need to be updated, maintained and repaired over time.

At its current level of development, AI is presently not in a position to replace humans, either now or in the near future. Additionally, to some extent it only functions according to the data it is fed, and although, it does learn from processing these, it is only to a limited extent. As such, current AI is not able to alter its response from changing environments the way that humans can. Finally, although it can learn over time from provided data and experiences, it lacks creativity for 'thinking outside the box' about problems[XXXII]. Many of this disadvantages contribute to limitations of the use of AI in organisations which are discussed later in this article.

4 HOW AI CAN BE USED IN SECURITY

To date, compared with other sectors, the use of automated technology in security has been relatively restricted, mainly consisting of linked applications for facial recognition and video analytics for alarm purposes[XXXIII]. However, in the last decade, with increasing availability of data (and in particular big data)[XXXIV], coupled with advances in computer capabilities, technology has helped the security industry to undertake certain tasks, previously carried out by a human workforce. This has been particularly invaluable where security resources have been overstretched, such as when labour shortages exist[XXXV].

Whilst AI in security is most readily associated with CCTV (or more correctly Video Management System VMS) it also has applications in other security technologies. But to do that it must go beyond merely collecting data and detecting events, to being able to supplement that data with data from other sources, detect patterns, identify connections, and inferences and then make decisions about the present, and predictions for the future based on these[XXXVI].

The rest of this section will consider specific examples of how AI technologies could help the security sector. Specifically, it will look at:

- Video surveillance
- Biometrics and facial recognition systems
- Access control systems
- Crowd monitoring
- Robot and drone patrols

Video surveillance

The security industry has long relied upon video surveillance to assist in undertaking a range of tasks, and recent advancements in AI-based operating systems have eclipsed the use of older legacy-based control systems, often made up of both software and hardware components[XXXVII]. AI-based video security is now more powerful, reliable and accurate, leading to faster response times to incidents and overall improvements in safety and security. One of the complaints about the old legacy systems is the number of false alarms raised due to incorrectly identified objects. AI systems on the other hand use algorithms that can be 'trained' to distinguish between people, animals, trees, and different types of vehicles, therefore, making it easier to spot potential threats and issues[XXXVIII]. Moreover, this intelligence continues to become more reliable and more accurate without any additional effort from the business, generating a good rate of return on investment[XXXIX]. Other benefits include real-time analysis of video footage, the ability to automate responses, and the elimination of the noise from a traditional monitoring system[XL].

Biometrics and facial recognition systems

The use of biometrics and facial recognition technology have long played a part in physical security, but the introduction of AI to these systems has greatly enhanced their performance. Whereas early biometric technology operated by using certain personal data relating to physical characteristics or markers, AI-enabled technology allows not only better recognition of physiological characteristics through 3D images, but is also able to distinguish between different behavioural characteristics, such as a person's movement or gait[XLI.] As well as tightening physical security systems for buildings and organisations, it can also be used for identifying perpetrators of crime, those on watch lists, airport services etc. and do so in a contactless manner[XLII]. This kind of use for AI (like those discussed further on) has however received some criticism, mainly relating to privacy concerns and therefore, legal standards need to be reviewed and revised to keep pace and scale with the developments of modern technology[XLIII].

Case Study 1 – Object detection using AI

Adopting AI technology can have a number of positive benefits for organisations, not least that it can increase their overall efficiency. By working 24/7 without interruption, breaks or downtime, compared to a human workforce, it can enhance productivity through making processes faster and smarter. It can perform repetitive tasks accurately, whereas humans might get bored, tired and lose concentration, leading to errors. Furthermore, AI technology can be deployed across a number of industry sectors and used at different levels of capabilities.

Besides assisting in routine and mundane jobs, it can also enable performance of more complex tasks, which is useful in decision-making, where not only does AI technology make decisions faster, filtering out some of the issues that might delay humans, such as emotional and practical factors, but it can use deep learning to handle vast amounts of data. This enables it to train itself and use this learning to categorise the data and build models to make more accurate future predictions. A further advantage of employing AI technology to undertake tasks is it can take risks rather than exposing humans to these. This could include using robots for defusing bombs and also in assisting governments and relief agencies by using data to predict natural and manmade disasters.

As noted, there are some disadvantages of using AI, not least that the start-up costs can be huge, depending on the level of intelligence and complexity an organisation is trying to achieve, the type of devices and software being used, and the amount and quality of data intending to feed the system. In addition, machines and technology will need to be updated, maintained and repaired over time.

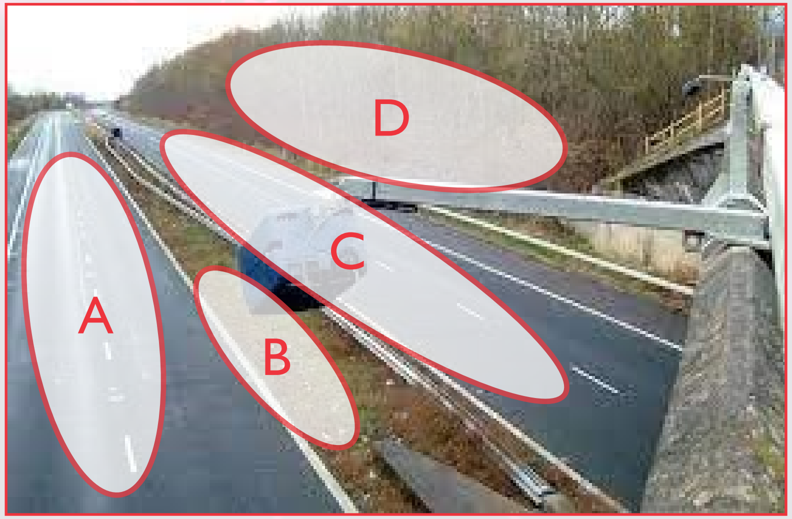
At its current level of development, AI is presently not in a position to replace humans, either now or in the near future. Additionally, to some extent it only functions according to the data it is fed, and although, it does learn from processing these, it is only to a limited extent. As such, current AI is not able to alter its response from changing environments the way that humans can. Finally, although it can learn over time from provided data and experiences, it lacks creativity for 'thinking outside the box' about problems. Many of this disadvantages contribute to limitations of the use of AI in organisations which are discussed later in this article.

Case Study 2 – Unusual activity detection using AI

Another use for AI with cameras is to determine if there is something different or unusual about the scene a camera is viewing. The camera learns what is normal by analysing the pixels it is viewing over a period of time, typically weeks or months and the longer it views the scene, the greater its ability is to detect a change to the norm. The picture below shows the view a camera would have if it was installed just as the dual carriageway was being opened to traffic. This is assumed to be an installation in the UK so the lane on the left will have vehicles travelling away from the camera and the right-hand lane towards the camera.

After a period of time the AI will have regularly seen groups of similar shaped pixels which it may or may not classify as vehicles moving northwards in area A of the scene, and southwards in area C, and at a greater frequency between 6am and 1am than between 1am and 6am. Area B typically has no movement at any time, but area D has movement at random times (such as branches moving in the wind). The camera will learn that these are the norms and the longer there are no exceptions to these rules, the more confidence there is in spotting exceptions. With those values learned, the camera would identify traffic moving in the wrong direction as an exception event, and any movement above a certain size in area B as another. It may also see a group of smaller pixels (smaller than a vehicle), such as a human in any area as an exception. Comparing movement against time variables is also important to fully utilise the detection of unusual activity at different times of the day, week and month.

Figure 2 – Views from a camera with AI installed on a UK dual carriageway



Access control systems

Many organisations already use automated access control systems as part of a solution to their physical security and integrating these systems with AI could take the detection potential to the next level. Indeed, during the pandemic there was an increased demand for touchless and frictionless access options, which not only gave organisations the ability to monitor who was accessing their sites, but also ensured that they adhered to any contact tracing protocols in place at the time. Intelligent access controls systems can monitor sites, protect sensitive data and diagnose problems, alerting human personnel to security issues in real time[XLIV.] One issue AI could assist further with is 'tailgating' or 'piggybacking'[XLV]. Although currently access systems can identify if it appears two objects break through the sensor, AI, through algorithms and sampling data, could further 'recognise' people through learned movements, patterns and features, virtually eliminating 'false rejections'. This would mean that systems could differentiate objects from humans (helping when people are carrying something or wearing backpacks) and could also be used to identify authorised/regular users[XLVI].

Crowd monitoring

Tracking and monitoring people for potential threats is a significant role for security personnel especially large crowds in busy streets, shopping centres, transport hubs or at events. But observing an individual's activity and behaviour is a near impossible task for the human eye alone and this is where AI can assist[XLVII.] By using a range of pictures and angles, machines can be trained to discern humans from objects and those images can be converted into data, where algorithms are then used to make determinations as required. As such, AI can automate some tasks to complement the work of security personnel like counting crowds and predicting issues. This was particularly important during the pandemic to ensure government regulations around social distancing were adhered to and has aided crowd control around the globe at large gatherings such as sports events, and other social and religious gatherings[XLVIII].

Robot and drone patrols

Security personnel are always on the lookout for potential threats, but where they are understaffed, lack suitable equipment, or in situations simply just too dangerous to investigate, gaps in security emerge. This is where AI can help, especially in the form of robot and drone patrols[XLIX]. Security robots have been used in the manned guarding sector for several years now, and can automatically patrol routes, detect strangers and objects, and transmit video and messages back to a monitoring guard. They have the advantage that where visibility might be limited, robots or drones may be able to detect issues, using sensors and thermal data, to give a more complete picture of a situation.

Where there are health and safety concerns, impeding human attention, robots and drones equipped with AI can assist in tasks, such as search and rescue missions, where toxic waste may be present, or helping maintaining law and order. They not only provide vital data and surveillance capabilities, but also give an expanded security presence in certain locations or situations[LI].

Although there have been some major advances in this field, especially in the last five years, there are still limitations using AI. For example, a robot is restricted to its functionality, and is unable to make judgement calls independently, which a human would be able to. In addition, their presence may be a bit conspicuous for certain environments, where more subtle form of security is favoured. Finally, although they can operate 24/7, they can cost significantly more to buy and operate, compared to human security guards[LII].

5 EXISTING CONSTRAINTS AND CHALLENGES USING AI IN SECURITY

Whilst AI has matured at a fast rate it does at present, possess some constraints preventing it from being utilised to its full potential, many of these are technical and processing issues, but other constraints exist too. Using CCTV as an example, firstly, technical and processing constraints are considered here, before moving onto more general constraints.

Technical and processing constraints

The utilisation of AI in CCTV is processor heavy with a great number of calculations required by what are, by their very nature, relatively low-cost devices. As such, there is a limit to the amount of processing capacity available, especially when this is carried at the edge[LIII]. To overcome this, most analytic engines will utilise a very low-resolution video stream to carry out the analytics, typically around VGA resolution of 640 x 480 pixels. Whilst using a low-resolution camera has led to the production of some powerful AI, it is true that being able to process higher resolution video streams allows more powerful and accurate analytics. A number of vendors now offer an additional "appliance", that is a standalone box which contains the analytic. These are typically available from 1 to 16 camera inputs and sit between the camera and the recording/monitoring location. This tends to be a camera agnostic solution with most cameras being capable of delivering a compatible video stream for analysis. This may be the primary video output or a lower resolution sub stream from the camera and overcomes the lack of processing power at the edge, without necessarily having to preclude the use of camera manufacturer specific compression techniques.

Bandwidth Constraints

Some AI solutions employ off-site/cloud-based storage and analytics as part of a recording solution. Whilst the video stream for AI (VGA) does not require a large amount of bandwidth, the "normal" output from a 4MP or higher camera will require substantial bandwidth to be transmitted to the cloud. A client investing in high resolution CCTV systems will have little incentive to "choke" the images to a lower resolution to achieve cloud connectivity. The cost, and in some cases actual availability of this bandwidth, will be a limiting factor in the processing of cloud-based analytics for an average commercial customer. For domestic clients with 1 or 2 cameras, this may be less of a limitation. However, this profile of user has little or no requirement for AI.

Storage Compression Constraints

The cost of storing data is relatively low and the ability to add more HDD into a storage solution is not onerous. However, there is still a growing market in vendor compression techniques with each vendor having its own method of encoding high resolution video into a low bandwidth stream, and de-encoding at the point of recording to overcome a low bandwidth transmission bottleneck. AI cannot typically work with this encoded video stream, especially if the AI provider is not the CCTV hardware manufacturer. This leads to a decision on the advantages of AI versus the cost of providing bandwidth and storage for uncompressed video.

5 EXISTING CONSTRAINTS AND CHALLENGES USING AI IN SECURITY

Algorithmic bias

Algorithmic bias in AI causes systematic and repeated errors by highlighting certain groups of data in systems, creating unfair and inaccurate outcomes which are rarely obvious. For example, a CCTV might have biases towards a subjects race or gender[LIV]. Bias may occur for a number of reasons, not just at the data training stage from particular preferences and exclusion, but it can also emerge as a result of how the data is used (especially for unanticipated or unintended use) or how outputs are interpreted[LV]. It may be unavoidable, in which case it is important to estimate the degree of the error (confidence interval) to interpret the results.

Regulation and privacy concerns

The regulatory environment in which AI operates currently does not sufficiently cover these new technologies, especially for legislation, monitoring, enforcement and effective remedies for harms. The issue of privacy has probably received the most criticism, with many claiming that AI is impacting on human rights through the lack of regulations and data protection, thereby also preventing the utilisation of AI to its full potential[LVI]. An example of this would be face detection where through GDPR regulations, individuals or organisations are not allowed to hold images (or electronic representations) of persons for civilian / commercial use, however, there can be exceptions to this if the AI is controlled or used by law enforcement or Government agencies. It is inevitable to some extent, that AI capabilities will constantly be in advance of a regulatory framework therefore, regulatory reforms will need to keep pace if the potential advantages of enhanced AI are to be utilised and public trust is to be fully gained.

Other constraints

In order for AI to continue to develop, it is important there is availability of quality data both for training and continued machine learning[LVII]. In the security sector, some suggest that physical security systems have lagged behind cyber security developments, because operators are overwhelmed with incoming-data and alerts, which are distracting and beyond what a human can handle, a similar situation which affected cybersecurity when first utilised. Physical security systems now need to be elevated to these standards if AI in this sector is to continue to grow, access to data from cloud technology is thought might help with this[LVIII]. The lack of skilled people is also a significant barrier to AI being adopted further, something that has been predicted for a number of years. In particular there is a shortage of machine learning modelers and data scientists, as well as for those undertaking data engineering and understanding business cases[LIX].

6 THE FUTURE OF AI IN THE SECURITY INDUSTRY

Although AI has greatly impacted our lives in the last couple of decades, compared to its potential, it has only developed a little, mainly because it is not able to get beyond mimicking human behaviour, and relies on being fed data. Therefore, even though experts expect security technologies to become more sophisticated in the future, few changes will probably be seen in the next decade[LX]. Whilst the previously discussed technical limitations will be improved with progress in each of these fields, these will probably be incremental, allowing AI to do the same things better and faster, but still doing the same things. For example, CCTV cameras will probably be able to "see" much further and with greater detail, but in the near future will not be able to process the input to arrive at decisions anywhere close to the speed and level of complexity a human can.

One clear trend, however, is the declining number of frontline security personnel (in part because there is a huge labour shortage), and as the number of these officers falls, the number of sensors in the industry is growing exponentially. Further AI capability and solutions therefore are desperately needed in this area because there literally are not enough humans to carry this out. Analysing video at scale in the next decade will be one of the primary uses for AI[LXI].

Robotics and drones will continue to be used in the security sector and this can be particularly beneficial where humans are unable to operate or where/when it is not cost effective to employ security officers. Although AI, especially in CCTV, is predominantly based around the sense of sight, as humans, we have many other senses we use consciously and subconsciously when understanding our environment. Therefore, it would seem a sensible development for AI to use as many senses as is practicable to give "multi-factor authentication" to what it is assessing, although this would need to be matched by ensuring privacy and human rights protection.

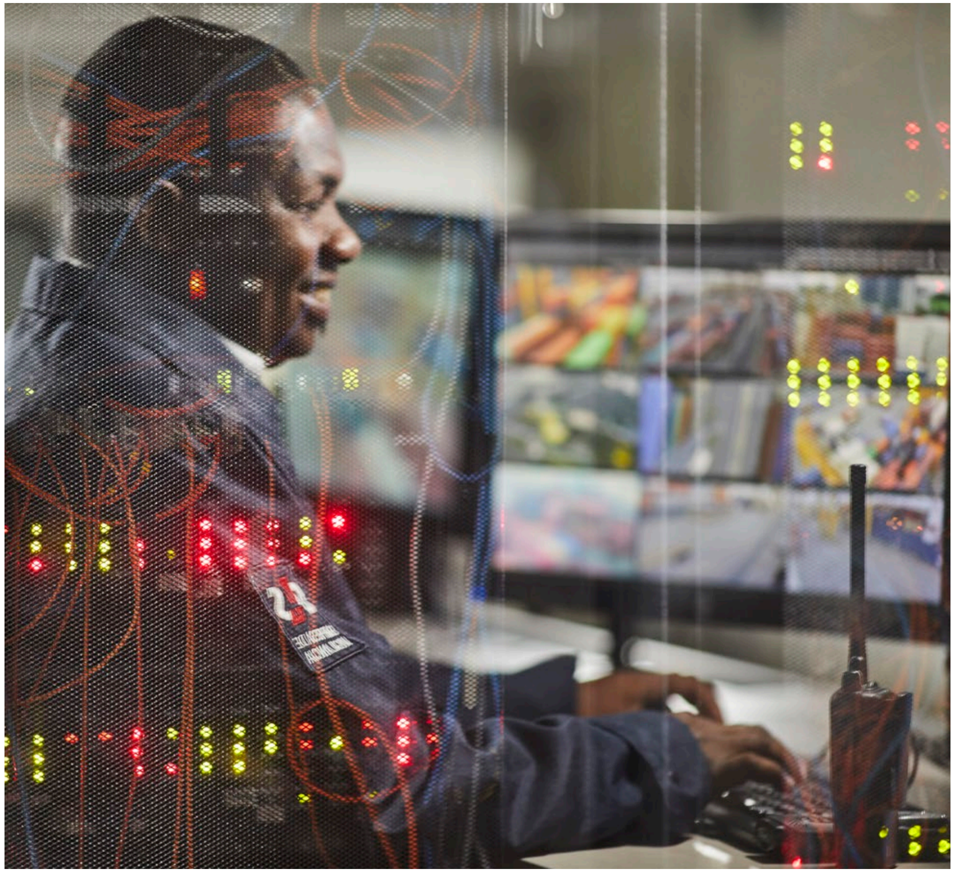
Other developments are likely to include further use of digital vehicle identification numbers (VINs), which allow vehicles to communicate with other systems. These can be used as part of a security system, and at some point, may be able to identify vehicles at a distance without reading the number plates[LXII]. The use of infrasonic and human natural vibrations (including those produced via a heartbeat, breathing and blood flow) are also likely to feature more greatly in AI systems, as they are specific enough to be determined as from human origin, thereby, assisting in deciding if an object is human or otherwise.

In the longer term, if AI gets to a stage where there is an extremely high confidence of accuracy in detection of an event or person it may then be able to take some next steps that are presently carried out by a human, acting upon the information provided. For example, presently if a person of interest to the police or similar is detected using AI, the act of informing the police is still the decision of a human. Whereas if via AI the certainty is 99.9%, and it may be the case even that AI can now be more "reliable" than a human in identification, then the AI may have the authority to directly inform the police directly. Simultaneously, the AI could dictate that any access-controlled door would not allow egress of the person of interest.

7 HOW G4S USES AI IN ITS PRODUCTS

G4S supports the use of AI and where appropriate, aims to use it in their security solutions. In particular, they heavily rely on the use of AI for remote monitoring and access control systems. G4S has partnered with Calipsa, whose cloud-based AI technology can instantly filter out true alarms, such as human or vehicle-based movements, from a variety of other motion triggers that could cause false alarms. Since bringing Calipsa onboard, G4S have seen false alarms reduced by 84%, allowing them to focus more time on genuine activations and less time on noise generated by false activations. ARC operator time is reduced through being able to target specific footage, meaning that true alarms can be prioritised. The impact of storms and similar on alarms, have seen a massive improvement, and operators no longer need to disturb customers in the middle of the night, which can sometimes be difficult conversations for both parties

Although AI in security is predominantly CCTV biased, there is emerging use in and operational access control and building management systems. G4S, in their AMAG Symmetry System offers a business intelligence module to monitor and flag behaviours or events that are out of the ordinary. This operates by learning what the normal behaviour of a building user is over a period of time. For example, a user might usually enter a building @8.30 am and leave @5pm Monday to Friday. If that person then starts entering earlier on a regular basis this could be an indication of a security risk (why are they in the building when it is empty?), or possibly a welfare issue (is the person overworked?). Similarly, if a person starts to regularly access an area that they do not usually (even though they have the right to access that area), the system will flag this change in pattern of behaviour for further examination. At no time is the system given the rules to apply, it uses machine learning to observe them over time, and then looks for anomalies to these to flag for further attention.



6 CONCLUSION

The use of AI technology in the security sector has certainly enhanced some tasks within the service, but its capacity is limited until such time it moves beyond computing, processing and applying rules (and in some instances generating those rule), to having the ability to react and respond to certain situations the same way that humans do. Security, by its very nature is dynamic, whereas AI by contrast, at its current level, is static and unchanging, seeing the world in black and white[LXIII].

Although AI will probably develop further in the future, until then, it will still need human input to interpret and respond to the issues it flags up in an appropriate way. Leaving this to machines purely could cause catastrophic incidents, as well as hindering the development of AI itself.[LXIX] It would only take one instance like this to push back development by several years and further erode public confidence. It is therefore important to ensure the benefits of AI are continued and further developed in the future that governments address regulatory and governance structures to ensure that the safety, privacy and the rights of humanity are fully addressed.

REFERENCES

I https://thedatacity.com/insight/four-ways-industrial-data-can-support-the-uks-ai-strategy/

II https://www.gov.uk/government/publications/ai-activity-in-uk-businesses

III Department for Digital, Culture, Media & Sport (DCMS) (2022) AI activity in UK businesses https://www.gov.uk/government/publications/ai-activity-in-uk-businesses

IV Gill, M. & Howell, C. (2021) Covid-19 and the implications for the security sector: what happened and what has been and is being learned?, Perpetuity Research https://perpetuityresearch.com/3658/report-launch-covid-19-and-the-implications-for-the-security-sector-what-happened-and-what-has-been-and-is-being-learned/

V https://view.genial.ly/606fc3a02fa7140d84dbf5f2/interactive-content-digestive

VI ASIS (2021) Opportunities and Implications of using Artificial Intelligence in the Establishment of Secure Physical Environments https://www.asisonline.org/globalassets/foundation/documents/digital-transformation-series/ai-guidance-document-final.pdf

VII http://www.differencebetween.net/technology/difference-between-ai-and-automation/#ixzz7PsylUp6y

VIII DCMS (2022)

IX https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence#:~:text=Artificial%20intelligence%20is%20the%20theory,making%2C%20and%20translation%20between%20languages.

X McPherson, S.S. (2018) Artificial Intelligence: Building Smarter Machines. Twenty-First Century Books, Minneapolis, MN, p. 4. What is Artificial Intelligence?

XI DCMS (2022)

XII https://www.auraquantic.com/artificial-intelligence-technologies-and-their-categories/

XIII DCMS (2022)

XIV ASIS (2021)

XV Hochreiter, S. (2022) Toward a broad AI. Communications of the ACM, 65(4), 56-57.

XVI Goertzel, B. (2007) Artificial general intelligence (Vol. 2). C. Pennachin (Ed.). New York: Springer.

XVII O'Carroll, B. (2020) What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence. Codebots. https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible

XVIII Pueyo, S. (2018). Growth, degrowth, and the challenge of artificial superintelligence. Journal of Cleaner Production, 197, 1731–1736.

XIX ASIS (2021)

XX https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=5c41faf233ee/

XXI https://bernardmarr.com/what-are-the-four-types-of-ai/

XXII https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/

XXIII https://machinelearningmastery.com/gentle-introduction-long-short-term-memory-networks-experts/

XXIV https://ieeexplore.ieee.org/document/8627945

XXV https://www.devteam.space/blog/theory-of-mind-ai/

XXVI https://meaxr.medium.com/self-awareness-in-ai-97a6a31c9a9e

XXVII https://www.hcltech.com/technology-qa/what-are-the-advantages-of-artificial-intelligence

XXVIII https://towardsdatascience.com/advantages-and-disadvantages-of-artificial-intelligence-182a5ef6588c

XXIX https://peak.ai/hub/blog/ai-decision-making-the-future-of-business-intelligence/#:~:text=AI%20decision%20making%20is%20where,to%20focus%20on%20other%20work

XXX https://www.lexalytics.com/lexablog/artificial-intelligence-disaster-relief

XXXI https://itrexgroup.com/blog/how-much-does-artificial-intelligence-cost/#

REFERENCES

XXXII https://www.proschoolonline.com/blog/what-are-the-disadvantages-of-ai

XXXIII ASIS (2021)

XXXIV Big data refers to data sets that are usually too large or complex to be dealt with by traditional data-processing application software and is often characterised by the 3V's – volume (size of database), velocity (speed at which it is processed) and variety (different data sources it is derived from)

XXXV https://www.ifsecglobal.com/physical-security/the-role-of-ai-in-physical-security/

XXXVI https://www.writeclick.co.il/the-role-of-artificial-intelligence-in-physical-security/

XXXVII https://artificialintelligence-news.com/2021/09/29/how-ai-video-surveillance-impacts-way-businesses-approach-security/

XXXVIII https://www.ifsecglobal.com/physical-security/the-role-of-ai-in-physical-security/

XXXIX https://artificialintelligence-news.com/2021/09/29/how-ai-video-surveillance-impacts-way-businesses-approach-security/

XL https://www.ifsecglobal.com/physical-security/the-role-of-ai-in-physical-security/

XLI http://www.ai.mit.edu/research/abstracts/abstracts2001/vision-applied-to-people/06lee.pdf

XLII https://www.innefu.com/blog/face-recognition-security/

XLIII Osoba, Osonde A. and William Welser IV, The Risks of Artificial Intelligence to Security and the Future of Work. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/perspectives/PE237.html

XLIV https://blog.boonedam.com/en-us/how-can-artificial-intelligence-improve-security-entrances

XLV Tailgating and piggybacking occurs when an unauthorised person gains access through a restricted barrier by closely following an authorised person

XLVI https://www.securityinfowatch.com/access-identity/access-control/article/21150569/how-ai-can-improve-security-entrances

XLVII https://www.getkisi.com/blog/6-ways-ai-will-change-physical-security

XLVIII https://dataconomy.com/2021/09/ai-best-solution-crowd-management/#:~:text=AI%20and%20Crowd%20Control,-So%2C%20where%20does&text=Engineers%20will%20use%20a%20diverse,determinations%20around%20any%20given%20requirement.

XLIX https://www.getkisi.com/blog/6-ways-ai-will-change-physical-security

L https://www.lorenztechnology.com/security-drone/?gclid=Cj0KCQjwjN-SBhCkARIsACsrBz4zMV-altlkYrrClnROat3IXTWXMhIr2dOe2oJ_PGhO__Nu2vzZx-YaAn8REALw_wcB

LI https://www.sourcesecurity.com/insights/artificial-intelligence-aiding-responders-natural-disaster-relief-co-14733-ga.1521629156.html

LII https://www.whatnextglobal.com/post/application-of-security-robots#:~:text=Physical%20Security%20Robots&text=Knightscope's%20robots%20can%20patrol%20the,crime%20based%20on%20visual%20images

LIII Recording at the edge allows users to record directly to a data storage card locally, rather than to a centralised system

LIV Introna, Lucas; Wood, David (2004). "Picturing algorithmic surveillance: the politics of facial recognition systems". Surveillance & Society. 2: 177–198.

LV https://www.healthcareitnews.com/news/how-ai-bias-happens-and-how-eliminate-it#:~:text=Bias%20in%20AI%20occurs%20when,how%20AI%20outputs%20are%20interpreted

LVI https://privacyinternational.org/learn/artificial-intelligence

LVII https://www.oreilly.com/radar/ai-adoption-in-the-enterprise-2021/

LVIII https://www.securityinfowatch.com/access-identity/article/21253250/ai-is-leveraging-advanced-analytics-for-physical-security-operations

LIX https://www.oreilly.com/radar/ai-adoption-in-the-enterprise-2021/

LX ASIS (2021)

LXI https://www.securityinfowatch.com/access-identity/article/21253250/ai-is-leveraging-advanced-analytics-for-physical-security-operations

LXII Rak, R., Kopencova, D., & Felcan, M. (2021). Digital vehicle identity–Digital VIN in forensic and technical practice. Forensic Science International: Digital Investigation, 39. https://www.sciencedirect.com/science/article/pii/S2666281721002328

LXIII ASIS (2021)

LXIV https://www.ifsecglobal.com/physical-security/the-role-of-ai-in-physical-security/

INTRODUCING THE G4S ACADEMY

We go far beyond simple security delivery.

Our G4S Academy is open to all those that operate in the security industry and provides a unique opportunity for networking, CPD and a constant stream of intelligence - such as our weekly threat intelligence report.

Our G4S Academy provides a monthly security bulletin on potential threats as well as a repository of white papers, webinars and other continuous professional development material

Our Events and Seminars where we invite guest speakers to debate the latest market evolution and trends

Our Innovation Forum where we work closely with our customers to discus new security issues and how best to address emerging trends and technologies

Our Podcasts support continuous professional development through engaging debate - available at your leisure

G4S Academy

G4S Academy

Noah Price introduces G4S Academy

INTRODUCTION

Listen to Noah's introduction and subscribe with our G4S Academy at https://www.g4s.com/en-gb/what-we-do/academy

G4S ACADEMY

UNITED KINGDOM › WHAT WE DO › G4S ACADEMY

Contact Us

UK: 08459 000 447
enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447
g4ssales@ie.g4s.com

G4S Academy