وزارة الداخلية
MINISTRY OF INTERIOR

ISNR
INTERNATIONAL EXHIBITION FOR
NATIONAL SECURITY & RESILIENCE

Preparing for the Future.

WESTLANDS
ADVISORY

Data. Insight. Strategy.

# The Rise of Artificial Intelligence: Impact on National and Cyber Security

From a technological and marketing buzzword to an increasingly effective tool that supports physical, national and cyber security operations.

# The Rise of Artificial Intelligence (AI): Impact on National and Cyber Security

## Table of Contents

The following Whitepaper will provide an overview on how AI is being used across security organisations, providing perspectives from both end users, government and industry. The paper will consider the following questions:

- What is AI and how has it developed?
- What are the benefits of AI?
- How is it being used in Security?
- How does it fit into security operations?
- What does the future of AI in security look like?
- What are the main challenges that AI will face?

# Introduction

2020 will be another important year in the development and growth of artificial intelligence. In 2019 AI started the move from being a technological and marketing buzzword to providing efficiencies and real value to operations across a range of industries. As it has started to prove its capabilities in other industries, there has been greater engagement with AI across security through testing, pilots and implementation across operations.

Artificial intelligence (AI) has been an established concept in technological science for over 70 years. The definition of AI is a contentious issue and organisations often use different interpretations to suit their needs. The Oxford Dictionary defines it as *'The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.'*

The table below gives an overview of some of the key foundations, applications and security themes that AI can deliver.

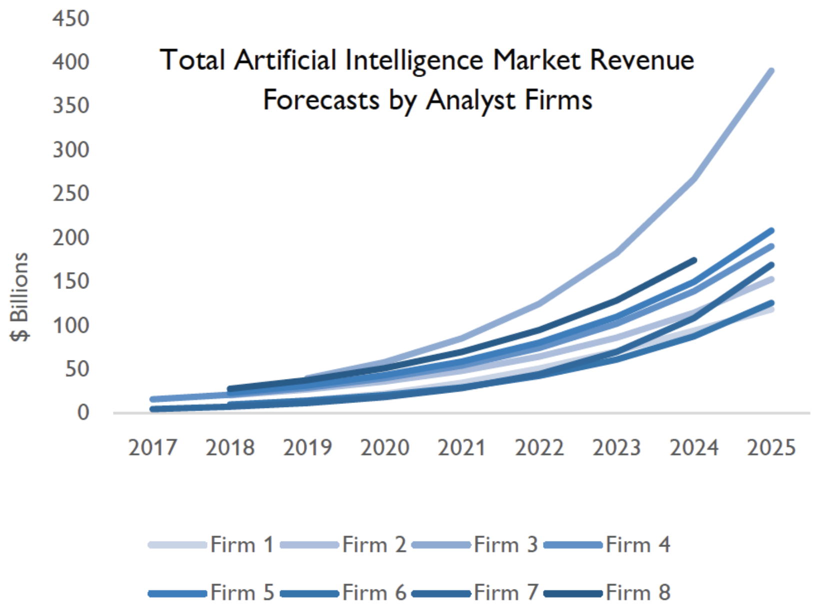
| Foundational AI | Applications | Security Themes |
|---|---|---|
| • Knowledge Graphs<br>• Rules-based systems<br>• Natural Language Processing<br>• Machine Learning<br>• Neural Networks | • Deep Learning<br>• Predictive Analytics<br>• Translation<br>• Classification & Clustering<br>• Information Extraction<br>• Speech<br>• Robotics<br>• Vision & Predictions<br>• Augmented Creativity<br>• Smart Automation<br>• Complex Analytics | • Data, Intelligence and Situational Awareness<br>• Speech to Text, Text to Speech & Conversational AI<br>• Machine Vision and Image Recognition<br>• Autonomous Vehicles<br>• Edge Based AI<br>• Cyber Security & Self Healing Networks |

There is little agreement on an exact definition, but it is widely accepted that there are different types and categories of AI. Narrow Artificial Intelligence is what is operational today and can perform specific tasks that outperform humans within set parameters. This includes assisted and augmented intelligence and usually requires humans in the loop, for example chatbots, facial recognition technologies and advanced analytics. General Artificial Intelligence is more advanced and broader and can function with humans out of the loop. It is able to complete cognitive tasks more quickly and more efficiently than humans, optimizing processes and tasks, increasing productivity and operational efficiencies, improving accuracy and providing intelligent advice from developing deep insights across multiple data sets.

Investment in AI from governments, major companies and start-ups across the world continues to grow. Pitchbook reported that in 2019 $31.8 billion deal value in AI start-ups across 2,899 deals.[1] Whilst this figure was lower than 2018, it shows the strength of investment, and does not take into account the ongoing efforts of larger companies such as IBM, Alphabet, Amazon, Apple, Nvidia and Microsoft or governments around the world.

[1] Pitchbook AI and ML tracking reported by VentureBeat: 03/01/2020

Westlands Advisory conducted an analysis of research and strategy firms that have tracked the market size and potential growth of AI over the next five years. There is a wide variance in the forecasts and how quickly firms think it will grow. However, all agree that it will be at least a **$100 billion market by 2025.**



As illustrated in the graph there is differing opinion in how much is being spent on AI. There is $250 billion difference between the highest and lowest forecast demonstrating the uncertainty of how quickly it will grow. However, with an average CAGR of 44% over the next five years there is consensus that growth will continue and the opportunity for AI to disrupt, enhance and improve operations is substantial. In addition, studies have shown AI can provide huge benefits to the global economy, with PWC projecting that by 2030 AI could contribute $15.7 trillion to the global economy.[2]

From a security industry perspective AI provides an innovative range of applications and benefits to enhance current technologies, and to better manage the increasing amount of data and support current operations to increase levels of security.

## Overview of the Security Industry

The global security market dynamics remain complex and continue to evolve. Shifting demographics, evolving social, political and environmental challenges are driving new and emerging threats. The growth of digitisation across security provides both challenges and opportunities. Digital technology enables collaboration, delivers efficiencies and facilitates the spread of information bringing significant benefit to business, governments and individuals. However, growing cyber incidents and attacks on digital infrastructure remains one of the primary threats across society.

[2] PWC: AI Sizing the Prize Report, 2017

Westlands Advisory has identified 10 trends that will significantly affect the security market over the next ten years:

1 Fighting the Digital Battle
Growing cyber security threats, information, misinformation and disinformation

2 Encouraging Collaboration
Multiagency collaboration, greater data sharing across governments and industry

3 Forced Migration
Conflict, insurgency and instability resulted in the largest number of displaced people in 2017

4 Innovating to Grow
Digitalisation will generate new value added services and transformation of business models

5 Two Trading Zones
Geopolitics, trade restrictions, business ethics and industrial policy will develop distinct trading blocks

6 Reducing the Noise
Risk and threat prioritisation tools will grow as the volume of data, information and knowledge builds

7 Corporate Risk Profile
Changing threat environment demands organisations have better detection and response plans

8 Complex Security Challenges
Increasing digital threats, changing criminal tactics, ongoing political and environmental challenges

9 Digitalisation & Autonomy
Rapid evolution of new and emerging technologies is enabling new approaches to security

10 Infrastructure Growth
$16.9 Trillion is expected to be invested in infrastructure 2019-2024

There are common themes across all these trends

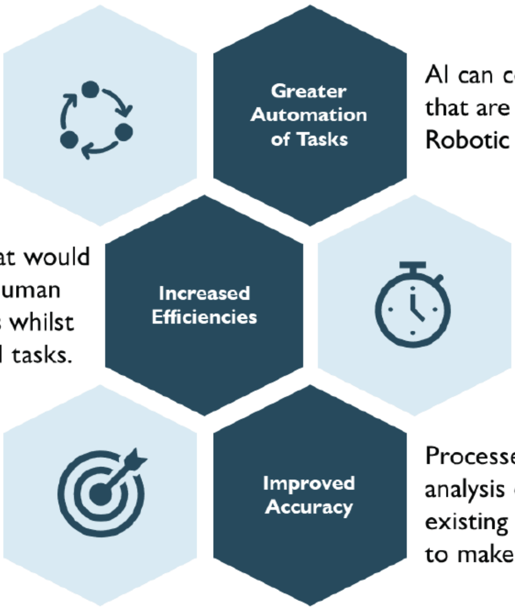
- **Digital Technology** – the growth of a more digital approach to security including growth of connected and data enabled devices from mobiles, radios, surveillance cameras and sensors gives greater information and situational awareness across security operations

- **Growth of Data** – digitization across society and increasing digital technology outlined above has created more data than security agencies are able to effectively manage. Data from open sources, internal databases, security technology and infrastructure are making the size and scale unmanageable for human interpretation.

- **Changing Threats** – national security threats including terrorism, organized crime and low level criminality continue to challenge security agencies. The nature of these threats and operations of criminal groups continues to adapt and challenge existing security. Cyber security is fast rising to the number one threat on organisations and government risk registers in terms of financial loss, criminal activity and potential disruption to critical services.

- **Pressure on Resources** – ongoing pressures on budgets and resources have driven security agencies to continue to challenge security agencies. The nature of these threats and operations of criminal groups continues to adapt and challenge existing security. Cyber security is fast rising to the number one threat on organisations and government risk registers in terms of financial loss, criminal activity and potential disruption to critical services.

AI can have a direct impact on many of these themes, and it will play a crucial role in how they evolve through delivering the following:



AI can complete repetitive and procedural tasks that are currently carried out by officers through Robotic Process Automation.

Analysis of huge amounts of data sets that would be impossible to do effectively through human resource, providing time and cost savings whilst allowing people to focus on other critical tasks.

Processes data to identify patterns that human analysis or advanced analytics may miss. Enhance existing systems to provide better information to make quicker decisions.

## AI in National Security

There is clearly a desire to use and integrate AI into security agencies operations. However, wide scale adoption has so far been limited.A core theme at the 2019 OSCE Annual Police Experts Meeting of over 130 security agencies and experts was the need to embrace AI to enhance efficiency and effectiveness.There has long been an acknowledgement that criminal organisations and individuals have used modern technology to facilitate their illegal activities and that law enforcement agencies need to engage better with technology to remain ahead of these entities. Some of the tools that are using AI that have already been tested include:

**Facial Recognition**

**Video and image analysis**

**Drones**

**Predictive Analysis**

**Robotics**

**Biometric Identification**

Levels of adoption and use of AI differs widely across security agencies around the world due to legislative, regulatory, cultural and social differences.What works in one region will not necessarily be applicable to others, however the potential power of AI is recognised throughout.There needs to be further debate about how to implement this into operations in an ethical, responsible and efficient way.

## Case studies

There are multiple examples of law enforcement and national security agencies using AI. Below provides a snap shot of some examples and the potential benefits that AI is already offering.

There are multiple AI pilots and programmes running in the USA. One of the most compelling is using an AI solution to help find and protect missing children. The FBI reported 465,676 missing children in the USA. A non profit organisation responsible for coordinating information and tips on their whereabouts received around 8.2 million tips a year. These had to be reviewed and prioritized by 25 analysts. Intel provided an AI solution that could use hundreds of thousands of past cases to learn and create a model to help identify valid and credible tips. This has helped track down missing children quicker, remove child pornography from the internet and the platform continues to learn and develop as the number of tips grow. It is expected to handle around 15 million tips this year.

Law enforcement agencies in the UAE have long used AI technologies as part of their operations. This has included creating a strategic plan for an Artificial Intelligence Department within then Dubai police. The plan focuses on delivering a comprehensive AI strategy by 2031 that includes smart police stations, AI assisted customer services, robotics, forecasting crime, crowd management and to enhance security across the road networks providing better traffic control. Many countries around the world are watching the implementation and tracking the success of these programs to learn how they may adapt them to their operations.

China has been one of the largest adopters of AI in law enforcement. This use of AI is fundamental to the Chinese 'Skynet Project', a national surveillance program that has led to the implementation of over 20 million cameras across the country. One of the best reported use cases is through facial recognition software developed by state-backed company, Cloudwalk. It is reported that the solution has led to the arrest of over 10,000 criminals in the past four years. The technology has been deployed in 29 provinces across China, it makes over 1 billion facial comparisons to its database each day and has accumulated over 100 billion data points. AI is at the core of the system to help analyse, identify and report information into real time operations rooms.

In the UK, AI is being used to establish predictive mapping programs, which interpret police data of past crimes, and identifies potential "hot-spots" or places of high risk on a map, in turn deploying officers to those areas of high risk. As well as this, UK police forces are utilising AI to create Individual Risk Assessment programs. These programs are predicated upon 34 pieces of data, 29 of which relate to an individual's previous criminal history. This gives individuals a risk score of low, medium or high based on the perceived threat that they pose. This programme is being used by Durham Police as a Harm Assessment

In addition to these there are multiple other opportunities. The European Emergency Number Association discussed a range of other AI use cases in a recently released paper that included the use of AI in emergency management. This included chatbots in PSAPs (Public Safety Answering Points), real time injury diagnosis and dispatch of Emergency Medical Services, video detection in crowded places for objects and subjects of interest in law enforcement and monitoring resources and equipment using AI and Machine Learning ensure the availability of critical personal protection equipment across a Fire Service.[3] Other applications include sentiment analysis to gain insights and better understand emerging trends on social media and to model weather patterns, flooding and natural disasters to help prepare emergency management agencies.

[3] EENA: Artificial and Machine Learning in Public Safety, 2019

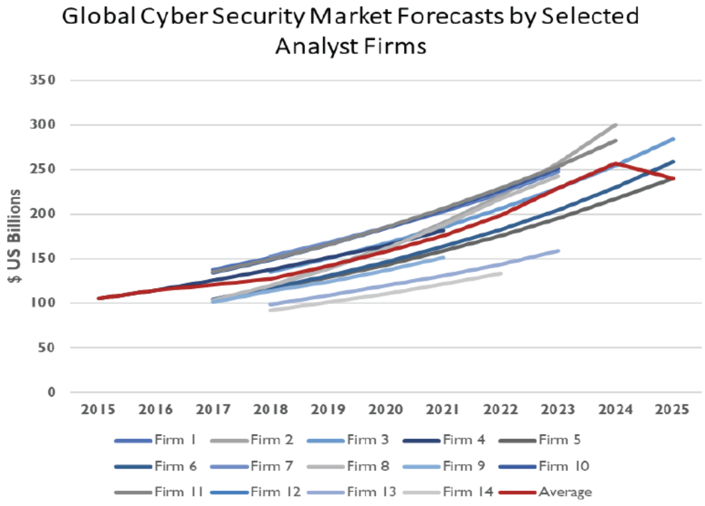
Although there are clear benefits to implementing AI across security operations, there are a number of challenges that also need to be considered. One of the biggest debates and challenges that AI faces is the debate around ethics. There have been many questions raised over fairness and accountability. Ensuring that the quality of data and information that forms the bedrock of AI learning and decision making is reliable, unbiased and nondiscriminatory to any people, group or organisations is vital. There are no quick solutions to this issue, and it is one that will have to evolve as the prevalence and capabilities of AI continues to grow.

Utilising AI in law enforcement has come under substantial scrutiny especially with regard to facial recognition and predictive mapping programs. Many of the UK police force have voiced their own concerns that AI is generating biased results. The concerns are that AI algorithms may judge people from disadvantaged backgrounds as "a greater risk" since they were more likely to have contact with public services, therefore generating more data that in turn could be used to train the AI. As well as this, predictive mapping programs have a tendency to deploy police officers to areas which are often subject to policing interventions that are disproportionate to the level of crime in that area – continuing the trend of bias and profiling.

## AI in National Security

Over the last five years cyber security has grown to be one of the greatest threats to governments and private organisations. The size of the threat continues to grow and outpace security measures and implementation. It is often quoted by security officials that a cyber security attack is not a matter of 'if' but 'when'. In 2018, Cisco reported that they blocked 7 trillion threats on behalf of their customers. According to Cyber Security Ventures, the cost of cyber attacks will be $6 trillion to the global economy by 2022.[4] These numbers give an indication on the scale of threat. Westlands Advisory conducted an analysis of the research and analyst firms that track the market size of cyber security. Whilst there are significant differences between the estimations, the strong message remains that cyber security will be the driving growth market in security and its growth will outpace traditional security and physical investment.

In 2019 the most conservative firm calculated a market size of $101bn whilst at the top end several firms estimated $168bn. The gap does not close over the forecast period with most firms calculating a compound annual growth rate of around 10-12%.



[4] Cybersecurity Ventures, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics," February 2019

Organisations simply do not have the manpower or budgets to deal with the size and threat, and so technology must play a large role. The use of AI is more mature in the cyber security market and is already acting as a key tool to help organisations better protect their IT and OT networks.

A recent survey of 850 IT executives, conducted by Cap Gemeni showed that 73% said they were testing use cases for AI in cyber security in some way, 8% of those were using products with AI embedded, with 30% using proprietary algorithms. The remainder use both proprietary and embedded AI solutions. 69% of the respondents claimed they would not be able to detect or respond to attacks without the help of AI, and that deploying it meant a lower cost to detect and response to breaches and enable a quicker response time.[5]

The main use cases for AI in cyber security include Network Security, Data Security and End Point and specifically to help with functions that include fraud detection, user / machine behavioral analysis, intrusion detection and malware detection.
It is important to note that this is one of the cases where the definition of AI becomes blurred. The terminology AI is used as an umbrella term for machine learning (ML) and deep learning, which are part of AI. There has been a strong growth in cyber products and using ML and deep learning as part of their solution and while these are not standalone AI products, they have started to integrate AI into their offerings. In the future we will see more cyber products that include AI either as standalone AI solutions or embedded as part of a wider product solution. The adoption of AI enabled products in cyber security will continue to rise.

## The future of AI in security

AI will continue to grow in applications across both national and cyber security operations and will remain a powerful tool to help enhance operations that support the security operations for governments, organisations and the wider public safety agencies. AI should be seen as a way to support ongoing operations rather than completely replacing them. Concerns over AI replacing jobs or leading to a reduction of personnel in security agencies should be dismissed. AI should be used and implemented to help agencies be more efficient and to provide a better service to the public, which fundamentally comes down to keeping them safer. It is expected that more pilot programmes, expenditure and implementation will see further growth over the next year. However, there are several challenges that must be addressed by both the suppliers of AI and the security agencies.

On 17th – 19th March the impact of AI in national security and many of the issues raised in this paper will be discussed at ISNR in Abu Dhabi 2020 and will continue to find answers to the following, supported by industry experts from public and private sector sharing latest innovations and best practice regarding the impact of AI in law enforcement and cyber security agencies' operations.

- How can we ensure the ethical development of AI?
- How can AI be responsibly implemented to support or improve security operations?
- What problem can AI solve in an operational environment that will provide increased security, better insight, efficiencies?
- How can industry and security organisations work together to get the most out of AI and the benefits it can bring?

[5] Reinventing Cyber Security with Artificial Intelligence: The new frontier in digital security: Cap Gemini Research Institute, AI in Cybersecurity Executive Survey N=850