Roke

Artificial intelligence and law enforcement

Achieving better outcomes through the use of AI within policing and law enforcement

The next few years will continue to see significant and fundamental changes in how law enforcement operates, underpinned by the increasing use of AI capabilities to aid better decision making and optimise the use of resources.

AI has the potential to transform the system, allowing operators to use it to target interventions, identify potential offenders proactively and effectively, predict crime hotspots, analyse CCTV images and more.

What is Artificial Intelligence (AI)?

AI is an algorithm or computational system that performs some cognitively complex action not usually associated with traditional software components. This includes machine learning (ML) algorithms; algorithms able to reason over complex and uncertain datasets, and algorithms that autonomously interact with complex physical or electronic worlds.

The technological capabilities of the police have advanced immeasurably since the days of COMPSTAT which was a combination of management, philosophy, and organisational management tools originally implemented in New York City in the 1990s. COMPSTAT represented a giant leap forward in the way law enforcement was able to make use of data science techniques, and is often associated with New York's rapid decrease in crime rates. Nevertheless, we've also learned some lessons about the pitfalls of a purely data-driven approach such as this.

Worldwide law enforcement agencies now have access to greater volumes of usable data and far more sophisticated and efficient methods of analysis. However, with this "explosion of data", from vehicle licence plate information and drone and body-worn camera footage, to digital images and text from online or digitally seized media, there's a need for law enforcement to devise accountable user friendly, intuitive, accessible and affordable systems that can process and analyse these quantities of data rapidly and accurately*.

Fact vs Fiction

In 2017 Google's AlphaGo unseated Ke Jie as the Go world champion, but the artificial intelligence behind AlphaGo isn't a great conversationalist – it can only play Go. Much of today's AI research is focussed on 'weak AI', which tackles specific problems, such as playing the game of Go. Weak AI has proven that its ability to learn surpasses the capabilities of most human beings and is able to achieve super-human performance levels on many benchmarks but it doesn't try to do everything a human can do. This means, for now, that we need to identify well constrained problems that AI can be applied to, and tackle them one at a time, often bringing knowledge from similar tasks that have already been 'solved'.

At Roke, we believe that there is a wide variety of law enforcement scenarios where AI could be used to augment operational capacity. These range from ensuring the safety of officers on the beat, supporting strategic planning in the boardroom, to improving operational efficiency in back-office functions. Law enforcement has the opportunity to use AI to exploit its vast operational knowledge to build a richer and credible intelligence picture, whilst maintaining public trust and a culture of partnership and interoperability.

Practically, if not used properly AI can introduce operational risk. Consequently, it is important that AI is built in such a way that users are supported to understand how it is doing its job, and trust the recommendations it is making – without, of course, needing to become AI experts! Validation, assurance and explainability are therefore critically important when using AI in the law enforcement domain. Developers must also take steps to protect AI against various forms of adversarial attack. Understanding the contexts in which AI can be adopted will help to ensure AI solutions move from proofs of concept into operational deployment.

To overcome these challenges Roke has developed an **Explain, Assure, Protect** methodology, which enables our clients to de-mystify AI, develop usable capability and train staff to realise all the benefits AI solutions can give them. To achieve this, we work with our clients and become their trusted advisor based upon our world leading combination of cyber, AI knowledge and consulting methodologies and skills.

Our Explain, Assure, Protect approach builds on fundamental principles

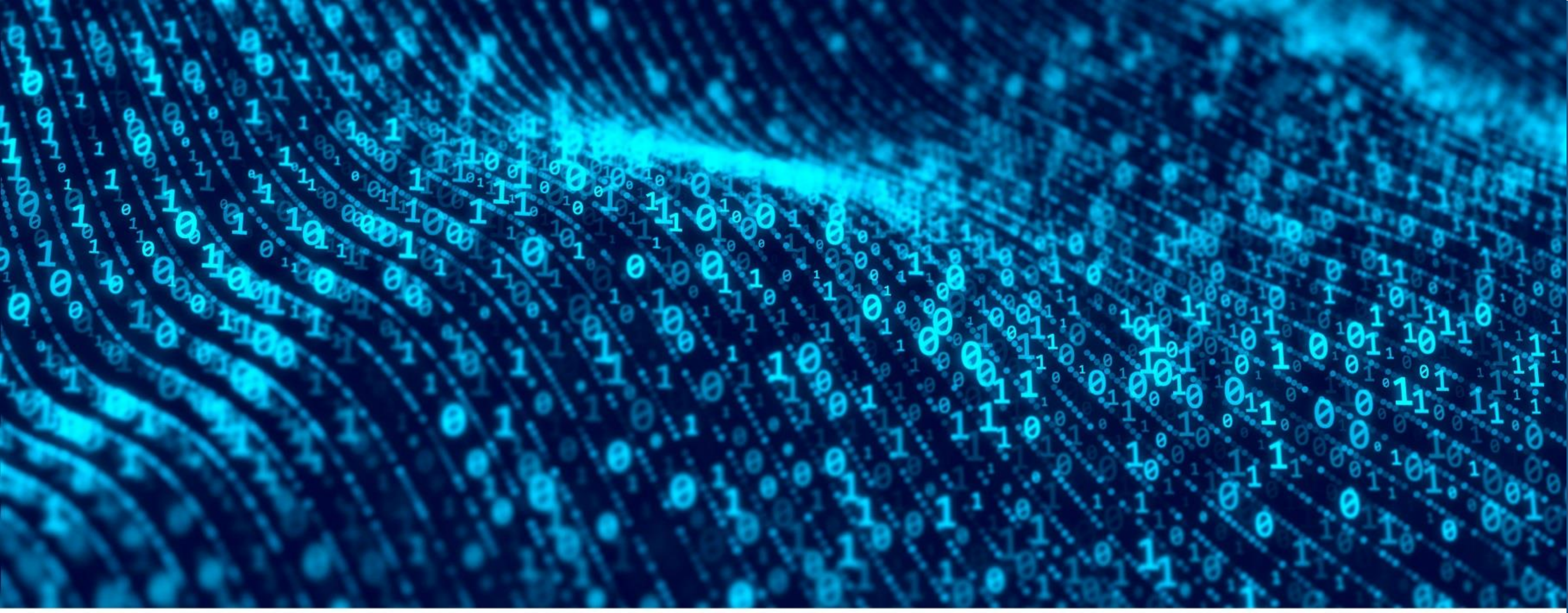
Explain: Our ability to articulate complex reasoning and decisions of AI components to our clients, so that the information provided is trusted and applicable to real-world scenarios. Explanations are critical for **ensuring trust** and for the ongoing assurance of AI. Without these and thorough training, the tools provided to make better and more informed decisions will not be used by investigators.

Assure: Encompasses the statistical and operational verification required to ensure the safety and effectiveness of AI. At its core, we ensure that the validation approaches and metrics used are robust and fit for purpose. AI may be required to reason safely over uncertain data or missing information and reasoning may be therefore unpredictable or subject to constraints. AI assurance includes understanding the constraints required to ensure safe operations and when it is acceptable or unacceptable to relax these constraints.

Protect: AI components have the potential to open new types of cyber security threats. Where an adversary is able to affect change in the training data used by a model, it's possible to 'poison' the model, making the AI less effective or incorporating loop-holes that might be beneficial to an attacker. ML models may be subject to 'reverse engineering', enabling an adversary to infer sensitive or classified training data. Finally, ML models may be subject to deliberate trickery through carefully crafted 'adversarial examples' that exploit weak aspects of the algorithm. Whether it be data inference, model poisoning, or adversarial examples; the risks and mitigations depend upon the operational use case and a holistic view of the complete system and its policies.

References

Babuta, Alexander. 2017. Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities. RUSI. P.20



Roke

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk   www.roke.co.uk

This publication is issued to provide outline information only, which (unless agreed by the company in writing) may not be used, applied or reproduced for any purpose or form part of any order or contract or be regarded as representation relating to the products or services concerned. The company reserves the right to alter without notice the specification, design or conditions of supply of any product or service.