DEFT can track a variety of targets, from multi-rotor and fixed-wing drones to naval vessels and land vehicles

Picture credit: Chess Dynamics

LOOK TO THE FUTURE

David Tuddenham *reveals how AI is being used for security tracking, resulting in a step change in capability*

We are moving ever closer to an era where all our movements are tracked by cameras that can analyse behaviours and predict potential threats. This isn't a dystopian plot, but a reality shaped by the advancements in artificial intelligence (AI) and its integration into tracking systems. And, while this technology is likely to enhance security, it also raises critical questions about the potential for misuse and the level of decision-making autonomy that can be introduced without adequate controls.

How do we ensure that these powerful tools are used in a way that delivers a step change in capability, while providing the level of real time controls required to prevent unintended consequences? In the defence sector, 'traditional' methods of targeting and tracking no longer meet the demands of evolving threats to global security. The emergence of agile, cost-effective and capable counter unmanned aerial vehicle (C-UAV) technology has accelerated changes in the defence industry and, when used by hostile actors in complex operational environments, state of the art applications can offer their operators a tactical advantage and pose a major security threat.

Overcoming this challenge requires advanced persistent surveillance that can maintain effective detection and identification with a low operator burden. This has been one of the drivers behind a rethink over how surveillance should be conducted – and this is where AI comes in.

AI can be programmed to sift through historical data as well current intelligence to predict enemy movements and strategies before they happen, allowing operators to anticipate future threats and start planning their countermeasures pre-emptively.

Advanced video tracking systems can follow targets over long periods, even in cluttered environments. This is crucial for tracking enemy movements, vehicles or drones.

Further, AI systems can process sensor data to identify and classify targets more accurately than human operators. This reduces the risk of friendly fire and increases the precision of military operations.

AI video tracking enhances border security by monitoring and detecting unauthorised crossings. It can track individuals or groups and alert security personnel to potential breaches. And, in search and rescue operations, video tracking helps locate and follow individuals in distress, even in challenging conditions like dense forests or built-up urban areas.

AI video tracking is extensively used in intelligence, surveillance and reconnaissance (ISR) operations. It has the capability to monitor significant expanses of terrain, identify potential threats – whether on land, at sea or in the air – and provide real-time situational awareness to operators.

Drones and other unmanned systems use video tracking for navigation, target acquisition, and surveillance. AI also powers autonomous drones that can perform reconnaissance missions. These systems can navigate complex environments and make decisions based on real-time data.

AI-powered drones and satellites can monitor huge areas autonomously, identifying and tracking potential threats and provide footage in real-time. They can analyse their own video feeds to detect unusual activities or movements and can process vast amounts of data from various sensors and cameras to identify potential threats and monitor activities in real-time.

AI can also be used in autonomous ground vehicles for reconnaissance missions, reducing the risk to human soldiers. These vehicles can move through hostile terrains and gather intelligence without direct human control.

The ethics of AI security tracking are complex and multifaceted, but some key concerns are bias and fairness. For example, AI facial recognition has led to false arrests of civilians after misidentifying individuals; and surveillance systems have been found to exhibit biases, which can lead to disproportionate targeting and surveillance of minority communities.

Jeena Joseph, writing in the journal *AI & Society* in August 2024, says: "AI systems do not merely reflect the biases of their developers; they actively shape our behaviours and perceptions in nuanced and often deleterious ways. For instance, consider the application of AI in law enforcement, where predictive policing algorithms identify potential crime hotspots and optimise the allocation of officers. At first glance, this approach appears pragmatic and data driven. However, these systems frequently exacerbate existing biases, resulting in an increased police presence in already heavily monitored areas… The ramifications of biased AI extend well beyond mere data inaccuracies; they impact lives and societal structures, perpetuating systemic inequality and injustice."

To work towards more equitable and reliable AI tracking, strategies for operating systems include incorporating data from various ethnicities, genders, ages and other relevant categories; focusing on detecting behaviours rather than identifying individuals; and establishing robust governance frameworks to oversee the development and deployment of AI systems.

To achieve these goals, systems should be monitored continuously by human operators and updated to address any emerging biases. This involves regular testing and validation against fresh data to ensure ongoing fairness and accuracy. Having diverse teams involved in the design and development of AI systems can help identify and mitigate biases from different perspectives.

Deep learning is a subset of machine learning that uses artificial neural networks to simulate the decision-making processes of the human brain. Deep learning can address AI bias through several key strategies.

Techniques like data augmentation can help create a more balanced dataset by artificially generating new data points. This can help mitigate biases that arise from imbalanced datasets. Regularly monitoring AI system performance and updating it with new data can help maintain fairness and accuracy over time. This involves ongoing validation and testing to ensure the model adapts to new patterns without introducing bias.

One of the most common applications of deep learning for video analysis is object detection and tracking. This involves detecting and tracking specific objects in a video recognition sequence. Popular techniques include the use of a convolutional neural network (known as a ConvNet or CNN) to learn complex patterns from data.

> THREATS CONSTANTLY EVOLVE AND SO MUST THE TECHNOLOGY TO COUNTER THEM

Such deep learning models are used in software for analysing video and detecting and tracking objects for trained classes, such as vehicles, ships, drones, or people, in real-time. More advanced video analytics software provides functionality for object counting and rule-based analysis, for example people-counting in areas with large crowds.

Another typical application of deep learning for video analysis is action recognition. This involves recognising specific actions in a video sequence or real-time video streams. Deep learning models can be trained to classify actions performed in different contexts or environments. More advanced methods apply video recognition or understanding, pose estimation, emotion analysis or face recognition to analyse and understand the context of video data.

Considering these innovations, video recognition and motion detection analysis are very popular for detecting activities in a scene by analysing a series of video frames.

Techniques for video motion detection or progress analysis include frame referencing or pixel matching to detect horizontal and vertical changes between a set of images or video frames.

Video tracking is now often preferred to alternatives such as infrared, due to its greater ability to classify its targets, but this has led to a greater expectation of video tracking to advance and meet the pressing demands of warfare and, considering the challenges discussed here regarding ethics and bias in AI, there is a need for a more 'hybrid' AI solution, which enhances the abilities of human operators and reduces the burden, without taking over from them completely.

In response, state of the art Deep Embedded Feature Tracking (DEFT) technology is already being developed and it is proving to be holding up effectively against new and evolving security threats.

Deep Embedded Feature Tracking (DEFT) is an AI-powered advanced real-time video tracking capability designed to provide accurate and robust tracking in complex situations. Chess Dynamics, for example, has installed DEFT on its newest CHARM Video Target Trackers, and the system uses its deep learning approach to optimise the identification and tracking of a moving target.

The technology has the potential to revolutionise surveillance, enabling reliable tracking of targets that are becoming increasingly difficult to follow. Threats can aggressively change appearance, helped by background clutter and other fast-moving and agile objects in the environment, but AI powered deep learning-based algorithms allow a comprehensive model to be made of the tracked target, enabling the system to accurately locate dynamic targets and reliably re-acquire them following periods of occlusion.

AI SYSTEMS CAN IDENTIFY AND CLASSIFY TARGETS MORE ACCURATELY THAN HUMAN OPERATORS

DEFT can track a variety of targets, from multi-rotor and fixed-wing drones to naval vessels and land vehicles and can do so with efficient autonomy. This means it can identify threats and enable automated acquisition and reacquisition of targets, while minimising false alerts. This reduces the burden on the operator to stare at a screen for long periods of time to detect and identify adversaries. The rapid and accurate identification of small, fast-moving threats is key to effective threat mitigation and protection of critical assets.

The technology creates comprehensive models of the target, allowing for continuous accurate tracking after occasional occlusion, for example. It provides for improved surveillance of difficult targets – an issue not unknown in C-UAS circles – in which traditional algorithms often struggle.

These models are continuously fine-tuned to enhance human user understanding of the target, resulting in precise long-term, robust tracking performance. The technology enhances the AI-driven target detection and tracking capability and integrates with neural network-based object detection and classification of targets.

As discussed, the increased proliferation of stealthy drones and more flexibly deployed forces has posed an unprecedented threat to security and privacy. These agile and hard-to-detect devices capitalise on cluttered environments to evade traditional surveillance methods, highlighting the urgent need for innovative technologies to counteract them. DEFT has been developed in response to this growing issue.

Threats constantly evolve and so must the technology to counter them, so our focus therefore must remain on continual enhancements that stay one step ahead of this changing threat profile.

Chess Dynamics is incorporating DEFT into smaller electro-optic systems and products while maintaining the high tracking performance of the technology. This will mean it can be integrated into autonomous platforms or installed within a camera to optimise performance of the automated video tracking and surveillance capabilities within a single device.

The multi target tracking ability of DEFT enables the system to measure the similarity between different detections and tracks to avoid confusion when there are multiple threats of the same kind in a small vicinity. Enabling effective multi target tracking on a device the size of a soda can is certainly a challenge, but such an enhancement is a key focus for defence leaders, and we are confident of further advancements in capability as we continue to invest in this product and technology.

There is huge potential for further innovation in artificial intelligence, and technology continues to develop exponentially to counter threats that seem to be adapting just as quickly.

Chess has already played a hugely significant role in this development and will continue to do so as we use AI to support and optimise operator and system performance ●

David Tuddenham is Group Managing Director of Chess Dynamics.

More advanced methods apply video recognition or understanding, pose estimation, emotion analysis or face recognition to analyse and understand the context of video data

Picture credit: Chess Dynamics