Picture credit: Patriot One

ARTIFICIAL INTELLIGENCE

Martin Cronin *examines the growing importance of the role of technology in security, potentially detecting threats before they occur*

Today's threat landscape is unpredictable and volatile, made even more so when set against the challenging backdrop of increased pressure on police forces, budget constraints, political instability and rising international threat levels. It cannot be denied that police and intelligence services are doing their utmost to protect society against the ongoing threat of attacks. But it may not be enough on its own. It demands a security response that is proactive, adaptable and dynamic. New technologies, such as artificial intelligence (AI), can dramatically improve the effectiveness of today's security systems.

Many current security measures that are relied on only offer retrospective intelligence and do little to prevent attacks ahead of time. The London Underground, for example, is monitored by surveillance cameras that prove invaluable when it comes to identifying individuals in the aftermath of attacks, as was the case with the London tube bombings of 2005. These terrorists were later seen on CCTV entering the station before the bombing.

There is a fundamental lack of systems in place that can detect a weapon or other active threat ahead of time. Instead, police are called to the scene after an attack has happened and are then reliant on the accounts of eyewitnesses or CCTV to identify and catch the assailant.

In order to better protect citizens, physical security measures need to become more proactive to the detection of threats before a tragic incident occurs. Technology is the key to achieving this. These new technologies can be used in conjunction with existing security systems to create stronger defences.

In many cases, reactive systems simply can't prevent loss of life. This is where innovations in physical security technologies come into play. By integrating existing CCTV systems, with AI-driven object-recognition software, detection of visible threats, such as guns or knives, can be realised before an attack happens and can help to minimise the horrific impact by alerting security and law enforcement in real-time of the location and nature of the incident. These new video capabilities can help fill the gaps that may be present in existing video management systems (VMS), so that on-the-ground security can be engaged sooner, to ultimately save lives.

Terrorists, particularly trained groups, are increasingly exploiting gaps in technology to plan and execute complex attacks, making it difficult for law enforcement to detect, intercept and stop. Furthermore, the increasing trend of individual assailants is becoming more challenging for security services to detect and prevent. In order to keep up with these challenges and protect ourselves most effectively, we must harness the latest advances in technology to ensure our defences can face up to the ongoing threats against us.

As referenced above with object recognition software for VMS systems, other recent advances are being driven by AI. Today, AI is leading the development of smart sensors that can not only detect visible threats, but also identify concealed weapons before attackers have the opportunity to use them. This breakthrough covert threat detection technology means the burden on law enforcement agencies can be lessened. Security personnel are better able to operate more efficiently by responding to a potential attack before it happens.

A particular benefit of using data-driven algorithms to identify threat objects, like rifles, handguns, knives and bombs, removes human bias in identifying suspicious individuals, helping law enforcement to feel more confident in their unbiased decision making. AI-enabled technologies can be completely objective in a way that is innately difficult for people. The benefits of this should come as a welcome relief for today's law enforcement who are constantly under scrutiny for profiling potential suspects.

The capabilities of today's physical security technologies are astonishing. Computer vision technology has existed for over a decade. Now, with the power of real-time AI software, integrated with current VMS systems, threat objects held in an assailant's hand can be identified for immediate response at schools, houses of worship, transportation hubs and event venues. This same technology can also learn the normal behaviour of a crowd in specific settings, so when unusual behaviour occurs, security can be alerted to pay extra close attention.

The AI approach to learning visible objects and human behavioural patterns can be applied to discovering those hidden threat objects, too. Using microwave radar and magnetic sensors to scan individuals and bags for threat objects and mass casualty weapons will not only protect individual identity, but also allow for security personnel to proactively address a potential threat before the weapon is even drawn or used.

There are also sensor technologies that can detect trace chemicals, like gunpowder, explosives and chemical agents, to parts per billion by 'sniffing' the air at a safe stand-off range; again, helping security track and stop terrorists before they act.

Using sensors to scan individuals for weapons allows security personnel to address a threat before the weapon is even drawn

DESPITE THE POTENTIAL OF NEW TECHNOLOGIES, THE ROLE OF PEOPLE MUST NOT BE DISREGARDED

All these technologies can be covertly deployed, integrated into a complete threat-detection platform within a security command and control operations centre, monitored by trained professionals. Combining multiple sensors into a single platform can provide an all-encompassing, proactive security approach, for a wide range of venues, such as schools, office buildings, event venues and transport systems. The result is a comprehensive, non-obstructive approach to safeguarding the general public from harm.

With the advent of so much technological innovation, we must also exert a certain level of caution. Despite ongoing global debate on the topic, there remains very little regulation about the use of AI in security. One thing is certain; it must be deployed in the right place, at the right time with the right objectives. People do not want to live in a fortress. They do not want to be protected by omni-present, overbearing security systems that infringe on their privacy.

Equally as important, the public recognises that it is important to be protected in its daily lives, and looks to local, regional and national governments to provide that support. New technologies can offer valuable and effective enhancements to public safety, but the right balance must be struck to ensure that we don't sleepwalk into a mass surveillance society.

Decision makers have to find a way to strike a balance between safety and protection of civil liberties and a layered, covert, multi-sensor approach to threat detection offers a rational solution. By deploying sensor technologies that detect weapons and active threats first, before individual identification, the public concern about living in a 'Big-Brother' society is mitigated. People don't have to surrender their privacy to ensure their safety.

As these new AI-driven technologies become more mainstream, some may question whether this new technology will have a negative impact on

security jobs. As Price Waterhouse Cooper estimates that 30 percent of jobs will be at potential risk of automation by the mid-2030s, it's a perfectly natural question to ask. However, like many industries, the solution is not mass redundancy and layoffs, but the evolution of new skills. Training to help current security staff utilise and work alongside these new AI-driven technologies, which can provide real-time information on the presence of a potential threat. It will be essential to maintain a well-trained workforce to successfully implement these systems and respond accordingly when alerts are triggered. Security staff should receive continuous training on policies and procedure, as well as guidance on how to identify behavioural indicators that may be apparent prior to attacks.

IT'S IMPORTANT TO HARNESS TECHNOLOGY TO ENSURE OUR DEFENCES CAN FACE UP TO THREATS

Despite the enormous potential of technologies that are beginning to transform the security industry, the role of people must not be disregarded. Technology can provide information and will alert security officers of a threat more efficiently, but it cannot negotiate with or physically stop an attacker. These technologies cannot reason with a disturbed gunman who is about to open fire on a school. These sensors cannot comfort the distraught, frightened parents of a young child who is lost in the chaotic aftermath of an attack. This is where the human element comes in. However advanced security systems become, the world will always need human engagement for action, as well as compassion and empathy, in moments of extreme crisis.

We need people, we need these new technology platforms, and we need policies and procedures working together to create safer public and private spaces. Technology on its own can only go so far. As a standalone solution, it is not the silver bullet to solving the UK's security problems.

In order to be most effective, technology must be embedded into national security policies and become an integral pillar of security training programmes. Decision makers need to have a comprehensive understanding of how to best implement and integrate the technology for it to be successful and effective. Collaboration and integration are key to creating a safer country. The emergence of smart and innovative solutions will arm today's security professionals with the tools they need to enhance and modernise security systems to defend against today's omnipresent threat ●

Martin Cronin, CEO & President, Patriot One is an expert in counter-terrorism, conflict resolution, and government/corporate interface. His career includes over 20 years' experience of international diplomacy with the British Government.

Technologies can be integrated into a complete threat-detection platform within a security control operations centre

Picture credit: Patriot One