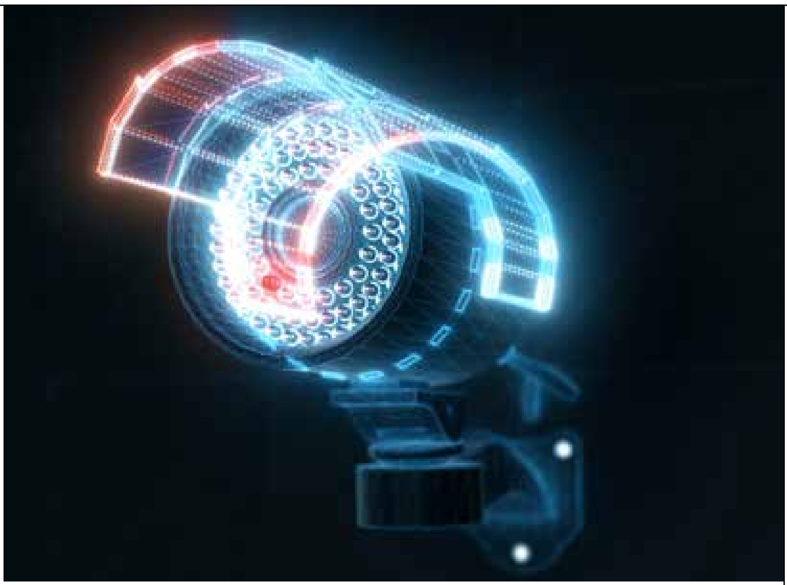
FROM AI TO ESG

Johan Paulsson *explores the six key technology trends that are set to impact the security sector in the coming year*



Advanced analytics can run directly within surveillance cameras on the edge of the network

Picture credit: Adobe Stock

Technology is pervasive in every aspect of our personal and work lives. Every new technological development and every upgrade brings new benefits, makes the tools we rely on more effective and creates stronger, more efficient services. But as technology's integration into society deepens, awareness of its implications is becoming more heightened.

Ours is an industry making use of increasingly intelligent systems with technology inherently involved in collecting sensitive data. It is also as impacted by geopolitical issues affecting international trade as any other sector. Security innovations will create a smarter, safer world, but in 2023 we will need to evolve to keep pace with these trends – all while moving fast to exploit new technological opportunities.

"From analytics to action" will become a mantra for 2023. AI and machine learning may have aided the development of advanced analytics in recent years, but the focus moving forward will be on exploiting the actionable insights they deliver. The huge increase in data being generated by surveillance cameras and sensors is a key driver for this transition. It is impossible for human operators to interpret the nuances of large data sets and act quickly enough, but analytics and AI functionality can now recommend, prompt, and even start to automatically take real-time actions which support safety, security, and operational efficiency in every key vertical.

Analytics can support new methods of post-incident forensic analysis using, for example, assisted search to automatically find desired video among massive silos of camera data. New techniques will also be used to predict outcomes, using sensors to propose preventative maintenance actions to minimise potential industrial outages before failure occurs.

Advanced analytics can run directly within surveillance cameras on the edge of the network. After-the-fact analysis, though, is a job for on-site servers or the cloud. Building the ultimate data analysis solution demands a hybrid computing architecture – and one which meets a customer's requirements precisely.

There is no perfect off-the-shelf configuration. Each business must assess its specific use case and define the hybrid solution that meets its needs. This process is complicated by localised requirements around data privacy and retention, which can force the use of on-premises storage over the convenience of the cloud, but architecture refinements are an essential part of any 2023 technology strategy. Businesses must maintain the flexibility to create the hybrid architecture best suited to their specific needs – architecture which can change as demand and future trends dictate.

Security hardware can present an opportunity to do more. Cameras themselves are powerful sensors capturing both quality video information and, thanks to advanced analytics, metadata which makes them useful in new and novel ways. Camera metadata can be combined with input from other sensors – monitoring temperature, noise, air and water quality, vibration, weather and more – to create an advanced sensory network and enable data-driven decisions. While we're beginning to see this kind of multi-sensor monitoring appearing in industrial and data centre environments, the eventual use cases are limited only by our imaginations – and platform-agnostic data streams enable bespoke applications for any use.

In the video surveillance sector, ensuring the authenticity and privacy of every data stream as it moves from camera to cloud to server is essential to maintain trust in its value. Cybersecurity is as vital today as it has always been, but 2023 will see a more proactive approach by technology vendors in identifying vulnerabilities, with bug bounty programs becoming even more commonplace to incentivise external parties to take a white hat approach. Customers will also increasingly expect transparency regarding the cybersecurity of security solutions, with a Software Bill of Materials (SBOM) becoming standard in assessing software security and risk management.

The compliance goalposts move regularly, and often with great speed. Each new regulation ratified brings a different aspect of software or hardware into focus. The European Commission's proposed AI Act, for example, aims to assign specific risk categories to uses of AI, and will no doubt be the subject of much debate before it becomes law. But whether in relation to AI, demands surrounding cybersecurity, data privacy, the influence of 'big tech' or tech sovereignty, it's clear that technology companies in the security sector will increasingly need to adhere to more stringent regulations.

KEY TARGETS FOR 2023

This is not a year of great upheaval – it's one of realignment. Our sector's greatest opportunity continues to come from focusing on commercial success in tandem with our responsibility to address critical issues facing the planet and its population. By working together towards a common goal, the combination of human inventiveness, advances in technology, and ethical business practices can be combined to make the world a better place ●

Johan Paulsson is Chief Technology Officer at Axis Communications