

From evolution to revolution

Security News Desk finds out how security solutions have been geared up to meet ever-evolving challenges.

Many of today's mission-critical security solutions are a far cry from what was fielded even ten years ago thanks to unprecedented, fast-paced, advances in technology and, crucially, the lessons learnt from the battle against terrorists - and criminals - seeking to exploit vulnerabilities in physical and cyber defences.

Stopping power

When talking about measures that represent the first line of defence against a determined vehicle-borne terrorist attack, hostile vehicle mitigation (HVM) is certainly high on the list. Given the changing threat landscape, vendors have, out of necessity, been driven to adopt more robust and innovative approaches here. In the UK, for example, the Glasgow Airport attack of 2007 was one of the events that acted as a catalyst for new thinking.

use by bomb disposal teams featuring: specialised robotic arms that provide multiple degrees of freedom; integrated payload bays, and the ability to deal with suspicious items in more confined locations.

Mark Kauchak, the Director of Sales and Customer Support at Northrop Grumman Remotec, tells me more about the added dimension that the latest robotic arms, for example, offer to operators who can control them remotely: "With [an arm's] additional degrees of freedom you are working more in three dimensions." Touching on other factors influencing EOD robot development, Kauchak continues: "We have seen increases in computing power and improvements in motors and communications. Ten years ago what was available drove robots towards a certain type of design but, with various advances, they enable you to do more and different things."

(Customs and Border Protection), stress that aerostats can offer a sophisticated form of persistent surveillance that other aerial platforms simply struggle to deliver.

Speaking to Matthew McNeil, VP Business Development, at US-based TCOM about the dynamics of aerostat development and the sensors they carry, McNeil replies: "As technologies that combine big data, analytics, and infrared and telecommunications, advance, lighter-than-air tactical aerostat platforms can be leveraged for ISR [Intelligence, Surveillance and Reconnaissance] applications." McNeil adds that technologies designed for the battlefield are also perfectly suited to address threats to 'the homeland' and can be readily applied to solve, and alleviate, the duties of domestic first responders.

Acti



integrated security management systems incorporating video, intrusion, perimeter protection and analytics, running on IT networks and infrastructures," explains Huysman.

Huysman believes that the emergence

From physical to cybersecurity

Of course any focus on the evolution of security would not be complete without referencing cybersecurity in some shape or form. With the move to IP-based video surveillance and access control solutions

Active CCTV algorithms

Turning to another aspect of security, the situation for video analytics is very much on the up as it starts to win adherents after a series of false dawns were, sadly, solutions were over-hyped and, when deployed, struggled to live up to their star billing. As times have changed, video analytics - or Video Content Analysis (VCA) - is being approached in a more accurate and down-to-earth manner.

One vendor has refined video analytics for retail outlets to the point where it can flag up specific behaviour around scan avoidance, at manned and self-checkout areas, with a high degree of accuracy. Interestingly, Malay Kundu, from StopLift Checkout Vision Systems - the leading player in this field - cut his teeth in facial recognition systems in airports and says that StopLift itself actually grew out of a Harvard Business School research study 'Project StopLift' on 'Retail Loss Prevention'. This was an effort which he reckons has stood him in good stead for the challenges found in today's retail environment: "We are applying a lot of really hard-core high tech here. That is how we are able to detect 'sweet-hearting' [where there is collusion between employees and customers] and generally scan avoidance. We are doing a ton of this kind of stuff for manned checkouts as well as self-checkouts."