ETERNAL VIGILANCE

Surveillance systems are a vital tool for intercepting terrorists and criminals – and automation is the key to increased effectiveness. ***Joe Charlaff*** reports on developments, including a US Department of Homeland Security initiative

After the attempted bombing in New York's Times Square in May 2010, no one can be in any doubt of the significance of surveillance systems. Very soon after the car was discovered, police had used surveillance camera footage from a nearby shop to identify a suspicious-looking man seen near the vehicle.

In the London transport bombings in July 2005, where 52 people were killed and 700 injured, police officials were able to trace almost the entire journeys of the four bombers as they prepared for the attacks, on dozens of surveillance cameras placed on the streets and in railway and tube stations.

Caught on camera

Security and surveillance cameras are everywhere today. But what happens to the footage they record? Often nothing, because there's no one to sit and sift through the endless hours of video. It's usually only after a major disaster or attack that officials check the video, hoping to get clues as to who or what caused the problem.

An Israeli company, BriefCam, is addressing the challenge of browsing the ever-increasing amount of video so that incidents may be investigated and identified more rapidly and action taken quickly.

BriefCam's Video Synopsis image processing technology is designed to allow users to review hours of video in minutes, or even seconds (depending on the number of events). Video Synopsis provides a very short video representation of the total footage while preserving the essential activities of the original. The synopsis simultaneously presents the multiple objects and activities that occurred at different times, with an index back to the source video.

Field tests conducted by a BriefCam client demonstrated that, on average, one hour of video review time could be reduced by up to 98 per cent – about one minute of viewing time for every hour of video.

BriefCam's president and chief executive officer, Dror Irani, says that industry response confirms that the company is on the right track: "Our list of technology integration partners keeps growing and we were awarded Best CCTV System Product of the Year at IFSEC 2010." The company offers an offline version of Video Synopsis for forensic investigation, and an online product that has been integrated to a list of partners that includes Genetec, Milestone Systems, OnSSI, Verint and Vicon.

BriefCam VS Online was recently installed at the headquarters of New York City-based Michael Stapleton Associates. MSA, a security consulting and services company with a strong client base that includes many Fortune 1000 firms as well as federal, state and local authorities, was one of the first security companies in the US to be designated or certified by the Department of Homeland Security (DHS) SAFETY Act.

The company is staffed by professionals from various backgrounds, including the NYPD's Counterterrorism Division, Emergency Service Unit and Bomb Squad, and from military service within specialised units. MSA provides specialised security solutions and training, domestically and internationally.

Recently, MSA expanded their service offerings with the Hostile Surveillance Program using video and physical analysis, and remote video analysis services.

The Hostile Surveillance Program was developed from a similar programme used by the US departments of State and Defense to protect US installations.

MSA's programme consists of an on-the-ground operative – a Hostile Surveillance Specialist (HSS) – who monitors critical surveillance areas for hostile activity and conducts an immediate follow-up investigation to ascertain the nature of the threat. The HSS is supported by MSA's Intelligence Analysis (IA) team, which provides intelligence analysis and a detailed understanding of the current threat environment.

MSA's HSSs make use of high-resolution CCTV cameras and are equipped with wireless communication devices fitted with hand-held remote video monitoring technology.

The HSSs are further supported by remote smart video analysis: specifically, Video Synopsis software developed by BriefCam.

Using BriefCam, MSA analysts trained in behavioural pattern recognition review multiple feeds of video footage over extended periods of time and assess people in the footage for behavioural anomalies.

BriefCam Video Synopsis also helps security departments to identify potential aggressors or other security concerns in the preliminary stages of casing and/or rehearsal before they act. MSA says: "The disruption of security incidents before they occur is the ultimate goal of any comprehensive security programme."

Prior to launching the Remote Video Analysis part of the MSA Hostile Surveillance Program, the software was installed and tested in the company's Security Technologies Center. This facility has been designed utilising a manufacturer-neutral infrastructure backbone that allows MSA to conduct new product and service research and development.

After testing BriefCam, MSA says it sees potential applications for the product that include: protection of critical assets and key resources; process evaluations for areas monitored primarily by CCTV due to the presence of occupational hazards; and other avenues such as loss prevention.

MSA's research team feels that Video Synopsis will help to expand their analysts' capabilities in reviewing cameras for clients, while reducing exposure to the monotonous process of reviewing video by more traditional means.

In January 2010, conversations between MSA and a financial institution led to the launch of a Hostile Surveillance Program in downtown New York City. MSA's analysts conduct daily research for tactical intelligence for HSS operatives in several fields, such as: protest activity or demonstrations at financial locations; changes in the terrorist threat environment; crime trends; other possible hazards (weather, traffic, etc); all-hazards intelligence briefings; review of HSS daily activity summaries; and daily co-ordination with military, law enforcement and academic threat analysts.

To date, MSA's HSS operatives have identified suspicious vehicles and pedestrians, probable protest groups, scouts and group intentions, potential crime suspects and other anomalies.

Networking synergy

Synectic Systems Group Ltd supplies integrated surveillance and security systems, specialising in long-range analogue, digital and thermal cameras with ranges of up to 13km. The company also provides radio monitoring and jamming systems, as well as portable surveillance and direction-finding systems for use in remote, hostile and quick deployment situations.

Synectic's digital recorders incorporate non-proprietary software that enables live and recorded video to be combined with a wide range of legacy third-party alarm or transaction-based system. Whether the system detects motion or intrusion, crowds, unauthorised access, abandoned objects, perimeter breaches, or even gunshots, the company's Synergy software is designed automatically to indicate the alarm location on a site map, present live associated video and recommend procedures to follow, and can even send a pager message to security personnel.

Jane's asked the company's joint managing director, Graham Jones, how he expects business to grow.

"We are seeing more government interest in protecting installations," he said. "Also, whereas security cameras used to be used for access, they are now used for an entire installation in protection of power stations, utilities, etc."

Jones pointed out the challenges involved with securing critical infrastructure in complex networks and applications. "Setting up sophisticated security systems takes time and is expensive. Where possible, it is desirable to re-use existing systems and only improve upon these where needed. This frees up budget, time and capability to install a more comprehensive system, thereby properly securing the infrastructure. The main complexity then becomes properly network-

ing and configuring these devices, which will naturally be from different manufacturers and according to different standards.

"Synectic's Synergy software and the hardware device it controls can pull all these data feeds together, control disparate devices, and even alert the operator when it detects suspicious activity. By handling all alarm systems and controlling all cameras and devices attached to it, it becomes the master security system.

The software provides features including video analytics through which advanced applications can be made, such as motion detection, tracking and automatic recognition of vehicles and people, people counting, and detection of abandoned objects.

"The main complexity becomes properly networking and configuring sophisticated security systems"

Border patrol

Controp Precision Technologies Ltd, a privately owned company based in Israel, specialises in the development and production of Electro-Optical InfraRed land systems (EO/IR) that are used for the purpose of border protection.

There are different systems for panoramic views, automatic intruder detection and intruder recognition. They are used in Israel along the borders as well as in other locations.

One of these command and control systems is the Spider, which is an EO/IR panoramic automatic intruder detection and recognition system. The Spider is a stabilised system, meaning that it can be placed on a tall pole or a moving vehicle, as opposed to an unstabilised system, which has to be placed on a permanent fixture, such as a building. When the system is stabilised the images produced will be clear, even if it is buffeted by wind on a high pole.

The system has an infrared camera (IR) for observation and scanning at night; a CCD colour camera that is used in daylight; a laser range-finder, which allows the operator to measure the distance to the target; and a laser pointer, used for target marking.

The system can operate on an autonomous round-the-clock scan with a very wide panoramic view and can scan back and forth without human intervention. The operator can monitor several screens simultaneously from the scans emitted from several systems.

The systems automatically detect intruders without the need for the operator to view the monitor at all times, or to actively perform any action. In the event of an intrusion, the system gives an audible warning so that the operator can then attend to the threat accordingly. If there is something suspicious, a security official can be sent out to investigate. This 'virtual fence' is a passive system without radio frequency radiation, so it cannot be detected.

The way the system is used for border control is that several systems are set up with the distance between them being the radius of the scan. They scan back and forth and overlap so that a long border can be protected. The multiple systems are operated from a command and control station set up in a convenient location.

If an intruder is detected, an audible sound is given. After sounding the alarm, it 'remembers' what it saw. The operator will then go into observation mode to take a closer look, but the system does not stop scanning and will pick up any more suspicious objects or intruders.

The system has different capabilities in order to reach maximum protection and provide a minimal number of false alarms. It is possible to mask out an area such as a farm, or an area that is assumed to be reasonably free of possible danger.

What is imperative is that the intruder is detected long before he reaches the real fence, allowing border control officers to apprehend him.

Lori Erlich, Controp's director of marketing and communications, told *Jane's* that there is tremendous growth in requirements as the 'bad guys' get smarter. "There is a definite upward trend in the development of unmanned systems as more efforts are being made to develop equipment that does not endanger personnel during surveillance operations."

Erlich pointed out that Controp develops systems in response to direct requirements the company obtains from people in the field. "We are meeting the challenges of surveillance operations and in that way helping to protect national security because we get feedback minute by minute."

Analyse this

Genesis EW, another Israeli company, has developed its GenCOM-HLS anti-terror solution functions based on data obtained from the cellular, satellite or wireless/radio communications signals of hostile elements. The system automatically maps and analyses the communicational behaviour of the suspects.

The main intelligence challenge is to 'find the needle in the haystack'; that is, to produce high-quality, real-time intelligence from the civilian communications taking place between terrorist parties, while overcoming the thick fog created by surrounding communication traffic running through civilian networks.

The GenCOM-HLS system provides intelligence consumers with new possibilities, insights and alerts thanks to continuous analysis of communicational behaviour and movement of suspects.

The applications include identifying, mapping and tracking of terrorist groups; dealing with an ongoing terrorist attack, including identifying the group members, the leader and the location of each one; perimeter defence of sensitive locations such as airports, seaports, crowded public venues and government offices; border control with alerts on approaching suspects; and assigning additional means, such as cameras, to control the event.

The system's capabilities include: detection of terrorist groups; mapping terrorist organisations' networks by analysing the interaction between known or suspected terrorists; real-time suspect tracking; locating the position of terrorists at any given moment; and detecting new ones through the suspects' interactions.

The system alerts the user as soon as the suspect acts, such as leaving the habitual geographical territory, deviating from the normal communication profile, or contacting a new or unknown individual.

Special event alerts are triggered when terrorists move to a sensitive area, convene with their peers or with members of other terrorist organisations, switch off their cellular phones, or approach the border.

As a 'learning' system, GenCOM-HLS can be fed with new patterns of terrorist organisations and act upon the new knowledge. Real-time monitoring and recording is carried out concurrently with an up-to-date display of the location of the communication devices to gain better, context-based insights.

A 'fingerprint' is obtained from transmissions intercepted automatically, with cross-authentication of the communication entities of a


sxc.hu/1365629

suspect and his contacts, in order to build a comprehensive communication profile of the target.

The fusion of data received from other sensors (such as still and video photography from security cameras or remotely piloted vehicles, or photographs and alerts from active resources) into an integrated display assists in validating the communications data and the detection of new patterns of terrorist activity.

The technology is based on lawful interception of cellular communications traffic directly from the cellular operators or off-the-air interception of communications through reception of cellular phones and cellular cells.

The system uses several location technologies: coarse cellular locating based on the distance of the phone from the cell and the strength of the signal in neighbouring cells, and accurate signal locating based on direction finders (DF) or based on time difference of arrival. A combination of approximate cellular location and accurate signal locating enables accurate locating with a 'fingerprint'.

The system is now being tailored to fit to border control scenarios in a western European country. In this case, the system will alert the border police to any unidentified emitters getting close to the border. The system is equipped with semi-active GSM (Global System for Mobile Communications) sensors and DF sensors, which can considerably improve the triangulation process. This is aimed at coping with the crucial need to detect emitters over vast areas.

Commenting on Genesis EW's expectations on market growth and development, Tala Cohen, chief executive officer, said: "From our recent experience with the market, there is a definite and distinct transfer from basic communication intelligence-gathering systems to summary communication intelligence systems. If intelligence consumers in the past relied mainly on systems providing communication interception, listening and transcription capabilities, today's consumers aspire to much more – they expect to have automated systems generating communication intelligence insights for them."

An extra pair of eyes

Traditional surveillance cameras can be of great assistance to law enforcement officers for a range of scenarios – canvassing a crowd for criminal activity, searching for someone who left a suitcase bomb beneath a bench, or trying to pick out a terrorist who has fled the scene and blended into a teeming throng in the subway. The disadvantages are that once they zoom in on a specific point of interest, they lose visual contact with the rest of the scene.

A new video surveillance system being developed by the US Department of Homeland Security's Science and Technology Directorate (S&T) may soon give law enforcement an extra set of eyes. The Imaging System for Immersive Surveillance, or ISIS, takes new video camera and image-stitching technology and bolts it to a ceiling, mounts it on a roof, or fastens it to a truck-mounted telescoping mast.

Like a fish-eye lens, ISIS sees very wide. However, that's where the similarity ends. Whereas a typical fish-eye lens distorts the image and can only provide limited resolution, video from ISIS is perfectly detailed from edge to edge because the video is made from a series of individual cameras stitched into a single, live view – like a high-resolution video quilt.

"This sweeping coverage with fine detail requires a very high pixel count," says programme manager Dr John Fortune of S&T's Infrastructure and a Geophysical Division. "ISIS has a resolution capability of 100 megapixels. That's as detailed as 50 full-HDTV movies playing at once, with optical detail to spare. You can zoom in closer without losing clarity".

The stitching together of several images isn't cutting-edge magic. For years, creative photographers have used low-cost stitching software to create breathtaking high-resolution images. But those are still images, created days or weeks after a scene was shot. ISIS is quilting video in real time, and a unique interface allows it to maintain the full field of view, while a focal point of one's choice can be magnified.

Further capabilities – many of them commercially available – will be provided by a suite of software applications called video analytics. One application can define a sacrosanct 'exclusion zone', for which ISIS provides an alert the moment it is breached. Another allows the operator to select a target – a person, a package, or a pick-up truck – and the detailed viewing window will tag it and follow it, automatically panning and tilting as needed.

Video analytics at high resolution across a 360-degree field of view, coupled with the ability to follow objects against a cluttered background, would provide enhanced situational awareness as an incident unfolds.

In the event that a terrorist attack has occurred, forensic investigators can pore over the most recent video, using pan, zoom and tilt controls to reconstruct the scene when it happened. Because these controls are virtual, different regions of a crime scene can feasibly be studied by separate investigative teams simultaneously.

Many ISIS capabilities were adapted from technology previously developed by the Lincoln Laboratory for military applications at Massachusetts Institute of Technology (MIT). With the help of technology experts from the Department of Energy's Pacific Northwest National Laboratory, Lincoln Laboratory has built the current system with commercial off-the-shelf cameras, computers, image processing boards and software.

ISIS's creators already have their eyes on a new, improved second-generation model, complete with custom sensors and video boards, longer-range cameras, higher resolution, a more efficient video format and a discreet, chandelier-like frame no bigger than a basketball. Eventually, the department plans to develop a version of ISIS that will use infrared cameras to detect events that occur at night.

S&T formed a partnership with the Massachusetts Port Authority (Massport) and, in December 2009, began an ISIS pilot at Boston's Logan International airport, allowing potential Homeland Security end users the opportunity to evaluate the technology. Beyond the potential for enhancing security at airports, if successful, the current testing at Logan could pave the way for the eventual deployment of ISIS to protect other critical venues.

That's a good thing, says S&T's Fortune. "We've seen that terrorists are determined to do us harm, and ISIS is a great example of one way we can improve our security by leveraging our strengths."

"Different regions of a crime scene can feasibly be studied by separate investigative teams simultaneously"