



DEMON breaks down the intelligence-sharing barriers

The ability to share intelligence between different police departments is as vital to modern policing as the introduction of fingerprint analysis in the 1890s. Nowhere is the need to share intelligence greater than in protecting and securing our borders. Yet the effective sharing of video and hi-resolution images has presented major problems – until now that is.

West Midlands Police secured 11 convictions following Operation Siluga, which made use of software suite DEMON, says Scyron CEO Michael Wilks (pictured).

By any standards it was a huge case. The riots in the Lozells and Handsworth areas of Birmingham involved 271 crimes, 2 murders and a staggering 5,000 hours of CCTV and video footage. With multiple defendants and a complex array of evidence, senior officers at West Midlands Police described it as one of the most complex investigations they had ever undertaken.

But officers working on the case, known as Operation Siluga, had an ace up their sleeve when it came to extracting, analysing, managing and presenting the video evidence. It came in the form of a powerful software suite called DEMON, developed by a UK company, Scyron.

The technology, which was developed with input from

West Midlands Police, helped secure 11 convictions. After the trial, Superintendent Una Cooke, head of the Major Investigations Unit at West Midlands Police said: "Without this technology it was felt that the case would have lasted at least another three weeks and, also, that it would have been extremely difficult for the jury to be able to follow the evidence against the individual defendants."

During the investigation multiple officers using different computers were able to work on the same video material simultaneously, with total visibility of each other's changes. The system helpfully kept a complete audit trail of changes. Video bookmarks and any notes made by officers were automatically flagged up. "Think

of review changes to a Microsoft Word document but to evidential standards and transferred to video, and you get the picture," said Michael Wilks, Scyron's CEO.

Following the success of Operation Siluga, Scyron developed DEMON Manager – a complete digital evidence management system – which allows police officers to work simultaneously on the same source material, and share that material across the department's network, whether it be video, maps, digitised documents, etc. Currently, the technology is in use with a number of police services, in major incident units, counter terrorism and volume crime. A big plus for DEMON Manager is its ability to scale rapidly. This is a crucial factor in major incidents where extra clusters of officers may be drafted into an incident room at a moment's notice and set to work at a terminal.

In responding to police officers' operational needs, Scyron had inadvertently produced major elements of what security services and the military now refer to as a "situational awareness" system.

Situational awareness

This latest buzzword is attracting a lot of interest in military and intelligence circles and from the likes of large software companies such as Microsoft. Yet, a quick trawl of the Internet reveals a confusing number of definitions. Put simply, situational awareness means being aware of what is happening around you to understand how information, events and your own actions and those of others impact your goals and objectives.

It processes four key elements (1) human, (2) important informational cues, (3) behavioural cues and (4) appropriateness of responses. For a fighter pilot this means being continuously aware of himself and his aircraft in relation to the dynamic environment of flight, any threats, and his mission goals, and then to be able to forecast and execute tasks based on that perception.

Although in use with the military, there are obvious applications for such systems in modern day policing. Complex investigations, like tracking down a serial killer spring to mind.

Thirty years ago such a system would have proved invaluable in the hunt for the Yorkshire Ripper. Its power would be in enabling officers to patch together information on attacks, potential and actual leads, suspects, locations, profiling information, etc.

While we are light years away from cranking the handle to deliver a prime suspect, in the Ripper case such technology could have enabled the police to pin point likely suspects or potential incident locations faster.

In the end, the serial killer Peter Sutcliffe was arrested in Sheffield after a routine inspection on his car revealed a false set of number plates. However, what the history books omit to tell is the extraordinary level of police manpower on the streets of Sheffield prior to his arrest. Studying his previous behaviour officers deduced that Sheffield was a potential future stalking ground for the killer. Yet this deduction only emerged over time and after the murder of 13 women.

The criticism levelled at West Yorkshire police eventually led to the development and implementation of the forerunner of HOLMES (Home Office Large Major Enquiry



The DEMON system identifies and learns the format required for video playback by a requesting officer, and adds it automatically to the police service's DEMON library.

System). The case proved to be a watershed and changed forever the relationship between policing and computing.

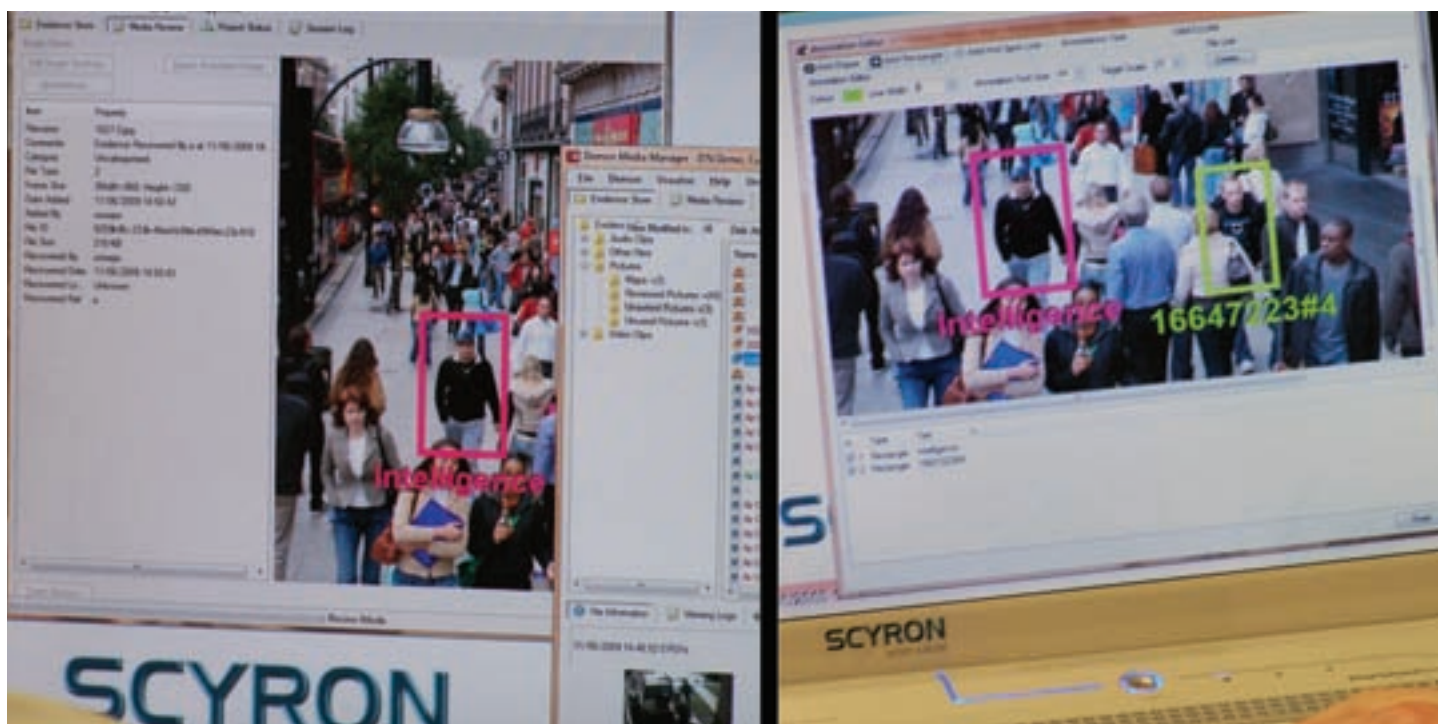
Today, information systems are an indispensable part of modern policing. And nowhere is the need more acute for them than in protecting our borders in the fight against international terrorism. Indeed, the global nature of the threat requires information sharing and cross-border collaboration on a scale unprecedented before the 9/11 attacks.

Yet terrorism is but one driver for enhanced border security. In an article on the CIA's website, Roger Z George noted, "It would be short-sighted, however, to focus exclusively on the 'terrorist' threat, as the world is now confronted with a host of border-spanning trends that challenge our traditional intelligence and law enforcement practices. International organised crime, narcotics trafficking, illicit sales of weapons – WMD as well as conventional – not to mention the spread of disease, internet-driven jihadist and other militant forms of radicalisation, and the geo-political implications of climate change head the list of new transnational challenges we are collectively facing."

The challenge of video and inter-agency intelligence gathering

While the requirement to share relevant intelligence on a timely basis has never been greater, it's not all plain sailing, as Scyron's Wilks points out. "The advent of video evidence has complicated matters greatly. If you think searching for and sharing video between police units in the same force was challenging, extending this to police services in other countries adds a new dimension of complexity."

As anyone who has tried downloading a large video file on the Internet will tell you, video is bandwidth hungry and can be frustratingly difficult to get working because of a plethora of player formats. In fact experts estimate



DEMON Enterprise was launched at ACPO-APA and it allows the system to run securely and encrypted over a Wide Area Network or the Internet.

that there are 6,000 different codecs in the world for video and CCTV.

Scyron set about solving the problem of transferring video through its DEMON Enterprise System, which enables officers to share digital intelligence across departments and geographies.

Unveiled for the first time at this summer's ACPO-APA International Policing Exhibition and Conference, the new system takes many of the features of DEMON Manager and allows them to run securely, and encrypted, over a Wide Area Network (WAN) or the Internet.

Wayne Phillips, global Defence Industry Solutions lead for the Public Sector, at Microsoft says: "Scyron has cracked the issue of extracting, analysing and presenting information from all kinds of digital information, including video/CCTV, photographs, scanned documents, audio and mobile phone evidence."

The system gets round the problem of transferring bulky video files by transferring a subset of information about the video, known as "metadata." For example, if a police officer has video footage of a suspected drug dealer meeting in a car park, they can send out the metadata, which contain stills from the video together with text information such as suspect name, location, time, etc. Much of the metadata is automatically generated by the DEMON system.

If interested, police officers in another location may request the video and even schedule a download time so as not to consume bandwidth resources and inconvenience other officers using the network.

Now let's assume that an officer downloads the video. Even if the format is obscure it can still be viewed immediately because the DEMON system identifies and learns the format and plays and adds it automatically to

the police service's DEMON library. This means any other officer, irrespective of which terminal they use, is able to play the files with that format in the future.

Wilks is almost evangelical about this new system and claims its real power is to join up different police departments and units in a way that has not been done to-date. "Imagine a beat officer who arrests a man breaking into a car and films the incident using body worn video.

The details of the man and video are captured by the system. If it later transpires the offender is a suspected terrorist, then that video becomes searchable to counter terrorist units. Information on him can be sent instantly to security services around the globe."

But it is not just joining the dots with video evidence that is important. Those tasked with protecting our borders are being equipped with a growing arsenal of technologies, such as X-Ray machines, thermal scanners, biometrics, listening devices, CCTV, etc. The need to capture, view, sort, index, store, retrieve, cross-reference, search and present this information is vital.

The scale of the task is massive. According to the UN, some four million people are smuggled across international borders each year. Equally alarming, Interpol suggests that the illicit global economy accounts for \$500 billion in world trade – about the same size as the combined GDPs of Hong Kong, Pakistan and the Czech Republic.

"International agencies need to be sharing electronic intelligence and video evidence to protect our borders," said Wilks, "but the same can be said of different departments within domestic police services – particularly with the rise of body worn video. Both are important. But I believe the latter is where the information revolution really starts."