Surveillance technology

If looks could kill

Oct 23rd 2008
From The Economist print edition

Security experts reckon the latest technology can detect hostile intentions before something bad happens. Unless it is perfect, though, that may be bad in itself

MONITORING surveillance cameras is tedious work. Even if you are concentrating, identifying suspicious behaviour is hard. Suppose a nondescript man descends to a subway platform several times over the course of a few days without getting on a train. Is that suspicious? Possibly. Is the average security guard going to notice? Probably not. A good example, then—if a fictional one—of why many people would like to develop intelligent computerised surveillance systems.

The perceived need for such systems is stimulating the development of devices that can both recognise people and objects and also detect suspicious behaviour. Much of this technology remains, for the moment, in laboratories. But Charles Cohen, the boss of Cybernet Systems, a firm based in Ann Arbor, Michigan, which is working for America's Army Research Laboratory, says behaviour-recognition systems are getting good, and are already deployed at some security checkpoints.

Human gaits, for example, can provide a lot of information about people's intentions. At the American Army's Aberdeen Proving Ground in Maryland, a team of gait analysts and psychologists led by Frank Morelli study video, much of it conveniently posted on the internet by insurgents in Afghanistan and Iraq. They use special object-recognition software to lock onto particular features of a video recording (a person's knees or elbow joints, for example) and follow them around. Correlating those movements with consequences, such as the throwing of a bomb, allows them to develop computer models that link posture and consequence reasonably reliably. The system can, for example, pick out a person in a crowd who is carrying a concealed package with the weight of a large explosives belt. According to Mr Morelli, the army plans to deploy the system at military checkpoints, on vehicles and at embassy perimeters.

Guilty

Some intelligent surveillance systems are able to go beyond even this. Instead of merely learning what a threat looks like, they can learn the context in which behaviour is probably threatening. That people linger in places such as bus stops, for example, is normal. Loitering in a stairwell, however, is a rarer occurrence that may warrant examination by human security staff (so impatient lovers beware). James Davis, a video-security expert at Ohio State University in Columbus, says such systems are already in use. Dr Davis is developing one for America's Air Force Research Laboratory. It uses a network of cameras to track people identified as suspicious—for example, pedestrians who have left a package on the ground—as they walk through town.

As object- and motion-recognition technology improves, researchers are starting to focus on facial expressions and what they can reveal. The Human Factors Division of America's Department of Homeland Security (DHS), for example, is running what it calls Project Hostile Intent. This boasts a system that scrutinises fleeting "micro-expressions", easily missed by human eyes. Many flash for less than a tenth of a second and involve just a small portion of the face.

Terrorists are often trained to conceal emotions; micro-expressions, however, are largely involuntary. Even better, from the researchers' point of view, conscious attempts to suppress facial expressions actually accentuate micro-expressions. Sharla Rausch, the director of the Human Factors Division, refers to this somewhat disturbingly as "micro-facial leakage".

There are about 40 micro-expressions. The DHS's officials refuse to describe them in detail, which is a bit daft, as they have been studied for years by civilian researchers. But Paul Ekman, who was one of those researchers (he retired from the University of California, San Francisco, in 2004) and who now advises the DHS and other intelligence and law-enforcement agencies in the United States and elsewhere, points out that signals which seem to reveal hostile intent change with context. If many travellers in an airport-screening line are running late, telltales of anguish—raised cheeks and eyebrows, lowered lips and gaze—cause less concern.

Supporters of this sort of technology argue that it avoids controversial racial profiling: only behaviour is studied. This is a sticky issue, however, because cultures—and races—express themselves differently. Judee Burgoon, an expert on automated behaviour-recognition at the University of Arizona, Tucson, who conducts research for America's Department of Defence, says systems should be improved with cultural input. For example, passengers from repressive countries, who may already be under suspicion because of their origins, typically display extra anxiety (often revealed by rigid body movements) when near security officials. That could result in a lot of false positives and consequent ill-will. Dr Burgoon is upgrading her software, called Agent 99, by fine-tuning the interpretations of body movements of people from about 15 cultures.

Another programme run by the Human Factors Division, Future Attributable Screening Technology, or FAST, is being developed as a complement to Project Hostile Intent. An array of sensors, at a distance of a couple of metres, measures skin temperature, blood-flow patterns, perspiration, and heart and breathing rates. In a series of tests, including a demonstration last month with 140 role-playing volunteers, the system detected about 80% of those who had been asked to try to deceive it by being hostile or trying to smuggle a weapon through it.

A number of "innocents", though, were snagged too. The trial's organisers are unwilling to go into detail, and are now playing down the significance of the testing statistics. But FAST began just 16 months ago. Bob Burns, the project's leader, says its accuracy will improve next year thanks to extra sensors that can detect eye movements and body odours, both of which can provide further clues to emotional states.

Until proved innocent

That alarms some civil-libertarians. FAST, they say, amounts to a forced medical examination, and hostile-intent systems in general smack of the "pre-crime" technology featured in Philip K. Dick's short story "The Minority Report" and the film based on it. An exaggeration, perhaps. But the result of using these devices, according to Barry Steinhardt, the head of technology and liberty at the American Civil Liberties Union in Washington, DC, will inevitably be that too many innocents are entangled in intrusive questioning or worse with "voodoo science" security measures.

To the historically minded it smacks of polygraphs, the so-called lie-detectors that rely on measuring

physiological correlates of stress. Those have had a patchy and controversial history, fingering nervous innocents while acquitting practised liars. Supporters of hostile-intent systems argue that the computers will not be taking over completely, and human security agents will always remain the final arbiters. Try telling that, though, to an innocent traveller who was in too much of a hurry—or even a couple smooching in a stairwell.